SECURITY DOCS DEPT.

THE AMERICAN MATHEMATICAL MONTHLY

THE OFFICIAL JOURNAL OF
THE MATHEMATICAL ASSOCIATION OF AMERICA, INC.

VOLUME 65 NUMBER 8

PUBLIC LIBRARY
OCT 31 1958
DETROIT

PART I

CONTENTS

The Washington Conference . . . . . H. M. Gehman 575
On a Certain Family of Arithmetic Functions . Paul J. McCarthy 586
Transformations of Integrals . . . . . Iain T. Adamson 590
Groupoids with Additive Endormorphisms . I. M. H. Etherington 596
The Concurrency of Perpendiculars . . . . . Paul A. Clement 601
Mathematical Notes. . Richard Bellman, P. C. Rosenbloom and . . . . . D. V. Widder, L. E. Clarke and James Singer, . . . Donald J. Newman, K. Venkatachaliengar, H. Hiż 605
Classroom Notes. . . . . W. A. Al-Salam, D. A. Kearns, ... L. O. Kattsoff, S. Leader, ... Herbert J. Curtis, G. E. Latta, W. Funkenbusch 615
Mathematical Education Notes 626
Elementary Problems and Solutions 627
Advanced Problems and Solutions 633
Recent Publications 638
News and Notices 651
The Mathematical Association of America 653
New Members. 653
May Meeting of the Indiana Section 656
May Meeting of the Minnesota Section 658
May Meeting of the Upper New York State Section 659
June Meeting of the Pacific Northwest Section 661
Calendar of Future Meetings 664

OCTOBER 1958

The AMERICAN MATHEMATICAL MONTHLY

(FOUNDED IN 1894 BY BENJAMIN F. FINKEL)

RALPH D. JAMES, *Editor*

ASSOCIATE EDITORS

RICHARD V. ANDREE	G. E. HAY	C. O. OAKLEY
JOHN A. BROWN	L. M. KELLY	J. M. H. OLMSTED
ROY DUBISCH	JOHN R. MAYOR	E. P. STARKE
HOWARD EVES	LLOYD J. MONTZINGO, JR.	H. S. ZUCKERMAN
	IVAN NIVEN	

EDITORIAL CORRESPONDENCE should be addressed to the Editor, R. D. JAMES, Department of Mathematics, University of British Columbia, Vancouver 8, Canada. Articles should be typewritten and double-spaced on 8½ by 11 paper. The greatest possible care should be taken in preparing the manuscript and authors should keep a complete copy.

ADVERTISING CORRESPONDENCE should be addressed to F. R. OLSON, Mathematical Association of America, University of Buffalo, Buffalo 14, N.Y.

NOTICE OF CHANGE OF ADDRESS by members of the Association as well as correspondence regarding subscriptions to the MONTHLY should be sent to the Secretary-Treasurer, H. M. GEHMAN, Mathematical Association of America, University of Buffalo, Buffalo 14, N. Y.

THIS IS THE OFFICIAL JOURNAL OF THE
MATHEMATICAL ASSOCIATION OF AMERICA, INC.

(Devoted to the Interests of Collegiate Mathematics)

OFFICERS OF THE ASSOCIATION

President, G. B. PRICE, University of Kansas
First Vice-President, G. B. THOMAS, JR., Massachusetts Institute of Technology
Second Vice-President, B. W. JONES, University of Colorado
Secretary-Treasurer, H. M. GEHMAN, University of Buffalo
Associate Secretary, LLOYD J. MONTZINGO, JR., University of Buffalo
Editor, R. D. JAMES, University of British Columbia

Additional Members of the Board of Governors: H. M. BACON, JEWELL H. BUSHEY, LAMBERTO CESARI, H. S. M. COXETER, P. H. DAUS, W. L. DUREN, JR., H. P. EVANS, HOWARD EVES, WILLIAM FELLER, N. J. FINE, J. S. FRAME, A. S. HOUSEHOLDER, G. B. HUFF, W. N. HUFF, G. K. KALISCH, E. C. KIEFER, J. C. KNIPP, W. G. LEAVITT, Z. L. LOFLIN, A. T. LONSETH, SAUNDERS MACLANE, J. R. MAYOR, E. J. MCSHANE, G. M. MERRIMAN, R. S. PARK, GEORGE PÓLYA, O. J. RAMLER, C. R. SHERER, M. F. SMILEY, R. G. SMITH, B. M. STEWART, F. M. STEWART, W. R. UTZ, JR., BERNARD VINOGRADE, CHARLES WEXLER, C. R. WYLIE, JR.

Annual dues for members of the Association (including a subscription to the American Mathematical Monthly) are $5.00. For non-members the subscription price is $6.00.

PUBLISHED BY THE ASSOCIATION at Menasha, Wisconsin, and Buffalo, N. Y., during the months of January, February, March, April, May, June-July, August-September, October, November, December.

Entered as second class matter at the post office at Menasha, Wis. Acceptance for mailing at special rate of postage provided for in the Act of February 28, 1925, embodied in Paragraph 4, Section 538, P. L. and R., authorized April 1, 1926.

PRINTED IN THE UNITED STATES OF AMERICA

THE WASHINGTON CONFERENCE

A conference to review the program of the Association and to formulate a plan of action was held at the Burlington Hotel, Washington, D. C., from May 16 to 18, 1958. The expenses incurred in holding the conference and in publishing its proceedings have been paid by means of a grant from the National Science Foundation. Invitations to attend the conference were sent to the officers of the Association, to the members of the Committee on the Undergraduate Program in Mathematics and of the Committee to Review the Activities of the Association, and to representatives of other interested groups.

The following thirty-three persons attended the conference:

E. G. Begle	Yale University
R. C. Buck	University of Wisconsin
E. A. Cameron	University of North Carolina
W. B. Carver	Cornell University
L. W. Cohen	National Science Foundation
C. W. Curtis	University of Wisconsin
R. L. Davis	University of Virginia
W. L. Duren	University of Virginia
H. P. Fawcett	Ohio State University
H. M. Gehman	University of Buffalo
R. D. James	University of British Columbia
B. W. Jones	University of Colorado
J. R. Mayor	American Association for the Advancement of Science
E. J. McShane	University of Virginia
A. E. Meder	Rutgers University
L. J. Montzingo	University of Buffalo
L. W. Nelson	Fund for the Advancement of Education
G. B. Price	University of Kansas
A. L. Putnam	University of Chicago
Tibor Rado	Ohio State University
Mina Rees	Hunter College
G. A. Rietz	General Electric Company
R. D. Schafer	University of Connecticut
M. A. Shader	International Business Machines Corporation
M. F. Smiley	University of Iowa
Rothwell Stephens	Knox College
R. R. Stoll	Oberlin College
Patrick Suppes	Stanford University
G. B. Thomas, Jr.	Massachusetts Institute of Technology
A. W. Tucker	Princeton University
E. D. Vinogradoff	President's Committee on Scientists and Engineers
S. S. Wilks	Princeton University
Dael Wolfle	American Association for the Advancement of Science

The topics discussed at the conference were grouped under these five headings: I. What the Nation Needs in the Area of Responsibility of the M.A.A.; II. Programs Required to Fill These Needs; III. Modernization of the M.A.A.'s Organization, Staff, and Headquarters; IV. The Funds Required; V. A Plan of Action.

Members of the Conference were invited to prepare working papers on topics coming under the above headings. Most of these papers were mimeographed and distributed to participants in advance of the meeting. Summaries of the prepared papers and of some of the discussions are given herewith.

Price: Purpose of the Conference. The purpose of the Conference is to study some of the problems created by the revolution in mathematics and to seek solutions for them. The revolution in mathematics and the rapidly increasing enrollments in high schools and colleges have resulted in unprecedented needs for mathematics teachers in high school and college, mathematicians for industry, preparation of students for graduate work in mathematics, modernized college mathematics courses, undergraduate programs for the training of mathematicians, textbooks from which the modernized mathematics courses can be taught, development of film and television aids to teaching, more efficient methods of instruction (such as the teaching of large sections), and expositions designed to help assimilate mathematical research into the body of common knowledge.

Besides considering the nation's needs in mathematics and programs which will help to satisfy them, some means must be found for initiating, organizing, operating, and supervising these programs. The Conference is to consider also the role of the M.A.A. as a professional organization and an operating agency.

The rapid growth of the Association in recent years has emphasized its strength and the appeal of its program, but growth has also brought problems. There are now approximately 7500 members, with a membership of 12,000 to 15,000 indicated by 1970. Approximately 23% of the members are now employed in business, industrial, and government positions.

The Association's program and responsibilities have undergone explosive growth, but there has been no corresponding growth in its staff, facilities, and ability to deal with its problems. The transition from an organization operated by a volunteer staff in donated headquarters space to one operated by a paid professional staff in rented quarters has begun. Nevertheless the officers of the Association are for the most part still chairmen of departments of mathematics. The Association needs leaders who have the time required to organize new activities and to locate the personnel and funds to operate them.

This Conference should study the nation's needs in mathematics and plan a program for the Association, and it should also seek ways to strengthen the M.A.A. so that it is equal to the tasks which lie before it.

Jones: Visiting Lectureship Programs of the M.A.A. Since 1954, the Association has administered, with the support of the National Science Foundation, a Visiting Lectureship Program for colleges. Its general aims are to strengthen and stimulate the mathematics programs of the colleges, to provide personal contacts with productive and creative mathematicians to staff members and students in the colleges, and to aid in motivating able college students to consider careers in mathematics.

A feature of the program has been its adaptability to local needs. In addition to formal lectures, each lecturer has conferred with students on future opportunities for study and employment, discussed problems of teaching and curriculum with faculty, disseminated information about what is going on elsewhere in the field of mathematics, and talked with administrators.

During the past four years there have been 16 lecturers, spending a total of 34 months on tour, and visiting a total of 270 institutions. During 1958–59 there are plans for 8 lecturers for a total of 14 months.

Visiting lectureship programs for high schools have been sponsored by the Kentucky and Northern California Sections of the Association, resulting in increased interest in mathematics among high school students, teachers, and administrators. The Association expects to sponsor a secondary school lectureship program on a wider scale starting in September 1958.

Buck: Mathematical Competitions. The reasons for initiating high school mathematical contests on a statewide or national basis are: to give official recognition by awards, presented in the name of the M.A.A., to some of the better students now taking mathematics courses; to discover and encourage talented students; to motivate students to

take additional mathematics courses; to encourage highly-gifted students to consider mathematics as a career; to give tactful guidance to the high school curriculum by indicating the level of competence that could be expected of the better students.

Several different types of examinations have been used to achieve these objectives. Since students differ in the amount of preparation, one method is to offer the contest at two levels depending on courses completed. Another solution is to devise a test which could be passed successfully by a very able sophomore, but could not be passed by an *average* senior with four years of mathematics. The Wisconsin Section has chosen this solution.

Two types of examination have been used: the *achievement* type and the *aptitude* type. The achievement type is characterized as a multiple choice test which attempts to measure a wide sampling of basic concepts and skills. The questions are of varying difficulty and are drawn from standard subject matter. It can be machine graded and is especially suited to a large-scale contest. The aptitude type is marked by an emphasis upon originality and insight rather than upon routine competence. It does not seem possible to design a multiple choice test of this type. This poses a difficult problem in the administration and grading of such a test where large numbers of entrants are involved.

A modification of the current national competition is proposed under which the contest would have two stages. The Preliminary would be held in February and would be a multiple choice test given in the high schools and proctored by local teachers. Since this test is to serve as a selection screen for the Final, the level should be set to select approximately the top 5% of the entrants. Statewide and local winners might be announced on the basis of the Preliminary examination. The Final Contest would be held at certain centers scattered through each state, usually at colleges and universities. This examination would be of the aptitude type. National awards and prizes of substantial value would be awarded on the basis of the Final Contest.

A summary was given of the Mathematical Olympiads of the U.S.S.R., the Eötvös Competition in Hungary, the Stanford University Competitive Examination, and the contests sponsored by the Wisconsin Section and the Metropolitan New York Section of the M.A.A., and by the National Committee of the M.A.A. in 1958 with the cooperation of the Society of Actuaries.

Discussion: Professor Rado stated that the problems in the Eötvös Competition were set by research mathematicians and that great prestige was attached to winning an Eötvös examination.

The Putnam Competition for undergraduates in colleges and universities was described as an example of an aptitude type of examination.

Meder: Textbooks. There are three types of courses for which syllabi, textbooks, and other teaching materials are needed: college freshman courses, major courses for prospective high school teachers, and other unconventional undergraduate courses. It would be an appropriate activity of the Association to issue a report discussing possible syllabi for freshman courses and the relative advantages of each; to appoint a committee to study the proper content for courses for prospective teachers and to make recommendations and prepare teaching materials; and finally to suggest and outline various types of unconventional courses. There is needed an overall directing committee, working committees in each major area, and specific production groups. Actual publication of the books written by these groups might be undertaken by the Association.

Begle: Textbooks. A writing group to produce a series of sample high school texts will assemble at Yale University in the summer of 1958. The group will consist of both high school and university teachers. It is hoped that first drafts of the texts will be completed by the summer of 1959 and that these texts will influence commercially-published books thereafter.

It is planned also to publish monographs on topics not ordinarily taught in the high schools. They are to be written by eminent mathematicians and are intended for the

better students, their teachers and the educated public. Texts for junior high school pupils will probably be written later.

Discussion: The need for both new textbooks and teachers manuals at the high school level was mentioned. The need for better preparation of prospective teachers was emphasized, as well as for upgrading of present high school teachers. Professor Fawcett stated that teachers are sincere and earnest in wanting to study more mathematics, but need special courses which are not often available.

Price: Summer Institutes. The National Science Foundation is supporting a major program of summer institutes for high school and college teachers of mathematics. In some cases demonstration classes of high school students have been employed with great effectiveness in conjunction with the institutes for teachers.

The institutes have been highly successful in accomplishing the purposes for which they were established. The participants have been brought into contact with current mathematics, and the encouragement and recognition they have received as participants have been highly stimulating.

Two trends have been observed which should be reversed: first, summer institutes for college teachers of mathematics have been almost completely eliminated; second, the number of summer institutes in mathematics, relative to the number in other fields, has been decreased. Because of the large number of high school teachers of mathematics and the importance of the subject, the percentage of institutes in mathematics is obviously too small.

If there should be a significant increase in the number of summer institutes in mathematics in 1959, the Association should stand ready to give help and advice concerning the planning, organization, and operation of these institutes.

Mayor: Summer Institutes. It has been estimated that there are 150,000 secondary school teachers of science and mathematics and that more than half of these are teachers of mathematics. This situation should be recognized in planning for summer institutes, and a much larger part should be institutes for mathematics teachers alone.

While it is true that in a considerable number of summer institutes mathematics courses were offered along with science courses, it appears that in many institutes a first consideration was for science. While all would recognize that it is important for mathematics teachers to study science as well as mathematics, it appears more important, in this time of curriculum modernization, that secondary school mathematics teachers be provided the opportunity in a summer institute to give their full-time study to the field of mathematics.

Discussion: Mention was made of other N.S.F. institutes, such as Academic Year Institutes and In-Service Institutes, also of institutes sponsored by industry, such as General Electric and Shell. It was suggested that a series of institutes be established, each emphasizing the applications of mathematics to one of the social or physical sciences.

Suppes: Some Possible Revisions of Mathematics Curricula. At Stanford University a course in calculus, not including foundations or set theory, has been given for behavioral scientists for the past four years. Emphasis is placed on probability, which seems to be most useful to the students, and which provides many nontrivial examples of application. Possibly material in probability theory will be introduced into the regular calculus sequence. Material on applications is needed for a number of other courses, such as matrix theory, where the students are mainly electrical engineers, physicists, and psychologists.

The acceleration of high school mathematics programs raises the problem of advanced standing in college. On the other hand is the problem of the large amount of remedial mathematics now done in college, particularly at state universities.

Finally there is the problem of the mathematical education of gifted children. Experiments are under way in the teaching of mathematical logic to sixth, seventh, and eighth

graders and in the teaching of plane geometry constructions to first graders. The present mathematical curriculum realizes a pitifully small part of the mathematical potential of the abler students.

Cameron: Undergraduate Honors Programs in Mathematics. Honors programs constitute one of the ways in which American colleges and universities attempt to solve the difficult problem of providing appropriate training for the more able students in a system committed to the education of all the people. Traditionally, honors programs have been limited to the upper years of college and they have consisted principally of a considerable amount of solitary study on the part of the student. There appears to be an increased interest in a rather different form of honors work.

Swarthmore has long been known for its honors work in several fields. More recently, Carleton and Dartmouth Colleges have inaugurated some very exciting honors programs in mathematics. These programs start with the freshman year and provide special attention for superior students throughout the four years of college. In these programs special work is not limited to individual study. The top students are together in classes or seminars with their peers for much of their work.

The importance of starting special work for gifted students in the freshman year should be emphasized. Many promising mathematics students have been lost by being subjected to dull and uninspiring first-year courses.

The Advanced Placement Program should have a direct influence on undergraduate honors programs. Talented students entering college with advanced training in mathematics constitute likely candidates for honors work. The proper education of superior students, from which group the mathematicians of the future must come, is surely a matter of great concern to us all.

Rees: Recruiting of Teachers of Mathematics. The extent of the need for additional teachers of mathematics was discussed. A solution is to recruit into mathematics those who are committed to teaching as a career but in a field where the need for teachers is less urgent. The long range problem requires that we interest more students in mathematics as a career, and that we provide better training for these students. We need better-equipped teachers who are assisted throughout their careers to remain alert and interested.

To interest more high school students in the study of mathematics requires beneficial relations between college faculty members and high school teachers. Even more important are contacts with high school guidance counselors, who need to be equipped to give sound advice to young people about the nature of a career in mathematics.

Another plan is to use lecturers to promote an interest in mathematics, especially lecturers from industry. Books and monographs afford another method for arousing interest.

Thomas: Expanded Programs at Meetings of the M.A.A. Five years ago the typical summer and annual meeting of the Association consisted of two half-day sessions either preceding or following the meetings of the Society. Since 1957 the summer meeting has been scheduled for four days, from Monday to Thursday, overlapping the meetings of the Society but avoiding conflicts with the general sessions of the Society. Similarly the Annual Meeting of January 1958 consisted of three sessions. The change in time of the Annual Meeting from December to January did not discourage attendance.

The reasons for the expanded programs of meetings is due to the increase in the membership of the Association, the broadening of interests of the membership, and the increase in the activities in which the M.A.A. is engaged.

Meetings of Sections are either one-day or two-day meetings. The variety of topics covered roughly parallels that at national meetings, with closer cooperation between college and high school groups, and, in particular, attention to matters of local responsibility and activity.

Meetings of the Association provide us with a variety of experiences. We renew

acquaintances, we talk shop, we make new friends, we become informed of what the various committees and projects of the Association are doing, we have the opportunity to learn something new in mathematics, and we may pick up some pointers on curriculum or on teaching which will make us more effective teachers. The longer meetings provide increased opportunities for us to realize the benefits of the experience just described.

Curtis: Expository Writing. It is suggested that a new expository journal be established under the auspices of the Association, each number to consist of a single article, to be self-contained, and to include a reasonably comprehensive account of its subject. Some articles should be aimed at research mathematicians, some at undergraduates or high school teachers. Substantial royalty payments should be made to authors.

It was also recommended that the Association publish lists of recommended books and articles with brief critical comments.

Buck: Expository Writing. Three separate expository series of books are suggested: Monographs of high-level expositions directed toward the active research mathematician who desires a survey of the present state of a restricted area of mathematics; college-level expository articles; high-school-level series.

Discussion: The concensus was favorable toward the idea of a journal or a series of books of the types discussed, but the difficulty in obtaining authors for the present Carus Monographs and Slaught Papers seemed to make it unwise to attempt to expand the present program of expository publications of the Association. It was pointed out that the most economical method of putting mathematical material into the hands of a large group was through publication in the MONTHLY rather than through the establishment of new periodicals or series of books.

In connection with expository writing, attention was called to the Chauvenet Prize awarded every three years by the M.A.A. for an outstanding expository article.

James: Publication Program of the M.A.A. The official journal of the Association, the American Mathematical Monthly, is issued ten times a year. Usually there is a supplement in the form of a Slaught Paper, although in 1957 there were two supplements, a Slaught Paper and the Dunkel Problem Book. The total number of printed pages (not including advertisements) was 760 in 1956 and 778 in 1957.

There is a waiting period of about a year for all accepted articles. This time interval is too long. Since the volume of mathematical material will increase, some thought should be given to the possibility of eliminating or reducing some departments of the MONTHLY.

The section on News and Notices, and the department of Official Reports and Communications of the M.A.A. might be eliminated or reduced in size. There is nothing in the by-laws that makes it mandatory to publish either the names of new members or reports of Section meetings. The question of the publication of book reviews that may be duplicated in other journals is a more difficult one.

The Association might very well consider increasing publication to twelve issues a year and including more 96-page issues. (The normal size is 80 pages.)

For expository articles, it would seem desirable to concentrate on expanding the series of Slaught Papers. It is difficult to persuade mathematicians to write expository articles, and it is by no means certain that payment for writing is the answer.

The editor is responsible for the acceptance of main articles, and the section editors for the material in their respective sections. It is clear that eventually the Association should have a central editorial office where the routine work of marking manuscript and reading proof can be done. Such an office will probably be required before the end of the term of office of the present editor.

Price: Facilities for Departments of Mathematics. The revolution in mathematics has greatly increased the needs of departments of mathematics for adequate department offices, offices for staff members, secretarial assistance, and special equipment and special facilities of various kinds. Buildings for departments of mathematics are still a rarity, and the problem of facilities for departments of mathematics is largely ignored.

Departments of Mathematics are asked to teach and to produce research. Research reports must be prepared and issued. Summer institutes must be organized and operated. Courses must be revised and text materials must be written and reproduced for class use. Staffs have become large and the administration of departments of mathematics has become burdensome. Proper facilities of all kinds would greatly increase the effectiveness of the nation's limited supply of mathematicians.

Davis and Tucker: Committee on the Undergraduate Program in Mathematics. The present committee has asked to be discharged as of September 1, 1958. It is expected that the committee will be reorganized on a larger scale.

During the five years of its existence, the committee has published four volumes of experimental textbook material: *Universal Mathematics* (two parts) and *Modern Mathematical Methods and Models* (two volumes). *Universal Mathematics* is now out of print but has been rewritten and will be available before the end of 1958. Artin's notes on *A Freshman Honors Course in Calculus and Analytic Geometry* have also been published by the C.U.P.

Gehman: Brief History of the M.A.A. The Mathematical Association of America was organized in December 1915 to cultivate collegiate mathematics (as contrasted with secondary mathematics and with mathematical research). It adopted as its official journal the American Mathematical Monthly, founded by B. F. Finkel in 1894. The object of the Association is, briefly, to assist in promoting the interests of mathematics. Membership is open to anyone interested in the field of mathematics.

With a Board of Governors of 42 persons, and 27 Sections with three officers each, there are (in spite of duplications) over 100 persons officially connected with the government of the Association. This is desirable; it encourages the feeling of loyalty that most members have for the Association.

Sections should be established in individual states, rather than having a Section include several states. As the number of Sections increases, a change in the form of government may be needed with an enlarged Executive Committee acting as a legislative body, and a Board of Governors consisting of sectional representatives and members-at-large acting merely in an advisory capacity.

It is recommended that the By-laws of the Association be amended as soon as possible to provide for the separation of the offices of Secretary and Treasurer. In time the Association will need a full-time paid Business Manager or Executive Director. In the case of the Editor, the Secretary, and the Treasurer, financial arrangements should be made with his institution to relieve him of part of his teaching load.

The Association holds various permanent funds, largely as bequests, whose income is used to support the publication program of the Association. The General Fund, amounting to $40,000, represents the surplus which has accumulated since 1915 because the cost per member was for many years less than the amount charged for dues. The cost of operation has been low because of the contributions of time and money made by many mathematicians. The magnitude of the operations now conducted by the Association requires more time on the part of its officers and hence requires greater financial support.

Mayor: Paid Executive Staff and Office for M.A.A. The recommendation that the M.A.A. establish a permanent, paid executive staff functioning under elected officers and a permanent nationai office in Washington is based on the need for a national organization, which will have as a principal purpose the improvement of mathematics education at the college level, and the need for a person in a full-time administrative position in Washington to represent mathematics. Many meetings concerned with science and mathematics education during the past three years in Washington have had no official representative of mathematics. This has resulted in mathematics failing to receive its needed share of attention in the development of programs.

Discussion: Wilks described the organization of the Washington office of the Ameri-

can Statistical Association. Cohen urged the establishment of an office of the M.A.A. in the Washington area. It was pointed out that the matter of public relations might be cared for through the establishment of a Washington office of the Conference Board of the Mathematical Sciences.

Stephens: The Role of the Sections in the M.A.A. A program by which the central organization might strengthen the Sections would include the establishment of a Vice-President for Sectional Affairs whose sole function would be to promote the welfare of the Sections. The MONTHLY should carry reports on important activities of Sections. Funds available to Sections should be increased. Each Section should be urged to establish a Committee to Study the Activities of the Section. The Association should recommend to the Sections speakers who are informed on and active in the Association's work.

Many of the Association's current activities have had their origins in the Sections, such as the contest for high school students, and the visiting lectureship program for high schools. But more can be done. Sections should interest themselves in providing increased facilities in mathematics for the gifted student. They can urge the establishment of courses, assist with Science Fairs in making mathematics an integral part of the exhibit, provide awards for outstanding college undergraduates, and can speed revision of the curriculum by sponsoring intensive courses on phases of mathematics not generally known by a good segment of the teaching profession.

Stoll: What is the Role of the Sections of the M.A.A.? At the organization meeting of the Association in 1915 three Sections were organized. Within ten years, seventeen Sections were in operation. At present there are 27 Sections covering all of the U. S. and Canada.

Section meetings show a great diversity in nature. The majority tend to offer a balance of talks on new mathematics, collegiate mathematics, and applied mathematics. Currently there is great interest and concern with high school mathematics and related subjects. A Section might indulge in self-help by providing that its members be well informed on the current emphasis in mathematical research and new applications of mathematics. It might help others by assuming an active role in the revolution that is currently underway in the high school mathematics curriculum. The program now under way in certain Sections to stimulate interest in mathematics and to encourage exceptional students in high schools could be greatly extended.

There are opportunites for a Section to perform a service at the state level by cooperating with state agencies and other scientific societies in overcoming existing deficiencies in the training of secondary teachers.

Mayor: State Programs for the Improvement of Science and Mathematics Education. It is probable that Federal funds will become available during the next few years to assist State Academies of Science in the development of programs for the improvement of science education. It is important that such activities include mathematics. Since many of the Academies do not include mathematics sections, some planning should be done to provide for cooperative programs involving the State Academies and the Sections of the M.A.A. It is recommended that the Sections seek opportunities to work in cooperation with other scientific societies and with State Academies.

Mayor: M.A.A. and National Council of Teachers of Mathematics. It would be desirable that these two organizations sponsor a number of joint committees and that they publish jointly certain publications of interest to secondary and college teachers. At least one annual meeting should be a joint meeting of the two organizations, and within the states, one meeting of the Section of the M.A.A. and the affiliated group of the N.C.T.M. should be held jointly each year.

Mayor: Membership. Substantial gains in membership of M.A.A. have been made in the past five years. Ways and means should be investigated to bring about an increase in membership. A few possibilities are: organization of special campaigns to be conducted by the Sections of the Association, joint meetings with other groups, solicita-

tion of membership during summer and academic year institutes, and by asking each present member to obtain one additional member.

RESOLUTIONS ADOPTED BY THE WASHINGTON CONFERENCE

A. *Resolutions on Institutes*

1. The Secretary is instructed to transmit the following resolution to the appropriate committees of the Congress:

Whereas the National Science Foundation has found it possible to support institutes for college teachers of mathematics and science only to an extent completely inadequate to meet existing needs, and

Whereas there is great need for these institutes both to bring about improvement in collegiate instruction and to undergird the recent widespread activity directed toward the improvement of secondary school programs in mathematics and science, and

Whereas institutes for college teachers may be considered essential in effecting improved preparation of new teachers of mathematics and science on all levels, therefore

Be it resolved that the Congress be requested to increase the discretionary power of the National Science Foundation in allotting funds for institutes for college teachers of science and mathematics, and

Be it further resolved that the Congress be requested to increase the funds available to the National Science Foundation so that this program may be instituted without detracting from the secondary school institute program, and

Be it further resolved that the Washington Conference support the request of the National Science Foundation for support of the expanded programs of institutes for teachers of science and mathematics.

2. The Secretary is instructed to transmit the following resolution to Dr. Alan T. Waterman, Director of the National Science Foundation.

Whereas more than half of the approximately 150,000 science and mathematics teachers in secondary schools in the U. S. are teachers of mathematics, and

Whereas, the needs of mathematics teachers are often inadequately met by combined science-mathematics institutes, and

Whereas, in the summer of 1958 only 13 out of 125 institutes are in mathematics, therefore

Be it resolved that the Washington Conference recommends that at least one-third of all institutes in the summer of 1959 provide complete programs in mathematics, under the direction of mathematicians, for mathematics teachers.

3. This Conference recommends that the President and the Secretary-Treasurer of the M.A.A. urge chairmen of departments of mathematics to submit proposals to the National Science Foundation for summer institutes in 1959, and supply them with information concerning appropriate proposals, programs, and staff.

4. Whereas this Conference believes (a) that the effectiveness of the program of summer and other institutes can be greatly enhanced if there is reasonable diversity in the objectives and programs of the several institutes, and the groups to be served by them, subject always to the fundamental principles that the institute programs shall consist essentially of the study of mathematics, and (b) that it is therefore important that institutions submitting proposals should give careful attention to formulating specific objectives for the proposed institutes and to the suitability of the program and staff for attaining them, and that the reviewing panels give weight to these matters; therefore

Be it resolved that the officers of the Association call these considerations to the attention of colleges and universities planning the establishment of institutes and urge the National Science Foundation to continue to judge proposals in the light of their stated objectives and their probable success in achieving them for the specific groups of teachers the institutes are planned to serve, and, indeed, to place increased emphasis

upon these considerations.
5. This Conference recommends that the President of the Mathematical Association of America appoint a standing committee on summer, academic year, and in-service institutes for mathematics teachers.
6. This Conference recommends to the Association's Committee on Institutes (when established in accordance with the preceding resolution) that financial support from the National Science Foundation or other foundations be sought, so that the functions of the Committee can be carried out without exclusive reliance upon volunteer activity.

B. *Resolutions on Programs of the Mathematical Association of America*

1. This Conference commends the work of the Committee on the Undergraduate Program in Mathematics, and urges that its work be continued with all possible vigor and on an expanded scale.
2. This Conference recommends to the Board of Governors of the Association that vigorous steps be taken toward more extensive publication of an expository nature, possibly including reprints of selected articles appearing in former issues of the MONTHLY and elsewhere.
3. This Conference recommends to the members of the Committee on High School Contests that they consider seriously the detailed proposals made by Professor R. C. Buck in his report on mathematical competitions, and requests that the date of the contest be much earlier than at present, not later than February 15 if possible.
4. This Conference recommends that a committee of the Association be appointed to gather and disseminate information about honors programs in mathematics.
5. This Conference recommends that a committee of the Association be appointed to distribute information about mathematics and employment in the field of mathematics to teachers, counselors and students in high schools and colleges. Especially should this committee initiate contacts with national and, through the sections, with local guidance and counselor organizations. Not only should written information be supplied but speakers should be suggested for meetings of these organizations. The publication of future editions of "Professional Opportunities in Mathematics" should be the responsibility of this committee.
6. This Conference recommends that a committee of the Association be appointed to organize and operate a Speakers Bureau. Such speakers should be drawn from business, industry, and government as well as from academic institutions and should be available to speak at secondary schools, collegiate institutions, civic organizations, and meetings of Sections of the Association. This committee should cooperate with the Sections of the Association in establishing similar activities on a sectional basis.
7. This Conference recommends that the Secretary-Treasurer request the Sections of the Association to appoint state liaison officers to deal with mathematical matters within individual states or provinces. A matter requiring immediate attention is the National Science Foundation program of support to state academies. The Conference also recommends that the Sections be urged to offer their cooperation to the state and regional academies in planning programs for which NSF support will be sought.
8. This Conference recommends that the Joint Committee on Places of Meetings invite the National Council of Teachers of Mathematics to hold its annual meeting at the time and place of the winter meetings of the Society and Association in 1960 or as early as is feasible.

C. *Resolutions on a Plan of Action*

1. This Conference recommends to the Board of Governors of the Association that the By-Laws of the Mathematical Association of America be amended so as to provide for a Secretary and a Treasurer, and an officer to be known as Executive Director, who shall be a full-time paid employee of the Association.

2. This Conference recommends that the office of the Executive Director be located in Washington, D. C., that an appropriate person be appointed to this position, and that funds be sought to support the position for an initial period of five years. The duties of the Executive Director shall be to serve as the executive officer of the Association, to carry out its policies and programs, and to serve as a liaison officer in promoting its activities. He should inform the Board of Governors of the Association of current problems and needs, desirable programs for meeting these needs, and governmental decisions affecting mathematics.

3. The Washington Conference recommends to the Conference Board of the Mathematical Sciences that the Board look to the establishment of an office in Washington coupled with the appointment of a suitable officer based there to deal on a national scale with problems and questions involving mathematics as a whole.

4. Whereas government, foundations and industry have begun to launch vast new programs of mathematical education in the public interest, and

Whereas these national and continental programs of mathematical education can be expected to grow and to involve much greater amounts of money in the future, and

Whereas the foundations and government have called upon the Mathematical Association of America to organize certain of these programs, to bring them into being, and to insure that suitable mathematical quality is maintained in them, therefore

Be it resolved that this Conference recommends to the Board of Governors a reorganization of the Association to include the formation of departments of management with men and money adequate to carry out the responsibilities assigned to them.

Specifically, special departments of the Association might now be recognized in the following existing activities:

(a) A Department of Periodical Publication charged with editing and publishing the American Mathematical Monthly, the Slaught Papers, and the Carus Monographs.

(b) A Department of the Undergraduate Program, charged with the Curricular work of the Committee on the Undergraduate Program in Mathematics, including the preparation of source material on new undergraduate courses, the urgently needed new courses for teachers, expositions, honors programs, and the promotion of curricular studies.

(c) A Department of Institutes, Visiting Lectureships, and Speakers.

(d) A Department of Competitions, charged with preparing examinations for national prize contests and conducting a service for operating such contests.

(e) A Department of Professional Guidance and Mathematical Manpower charged with the preparation and publication of guidance material on mathematical manpower and the promulgation of information on mathematical vocations and training for them which is needed by school guidance officers and industrial employment agents.

The establishment of these departments of management should meet the following requirements.

(A) Each department should have a charter approved by the Board of Governors which defines its sphere of activity. Each department should be responsible to the Board of Governors through a committee with appropriate provision for limited terms of office and rotation, including representatives of Canadian collegiate mathematics where appriate.

(B) Each department should have a Chairman whose position is guaranteed by the Association to be stable, to have professional status, and to carry a full or part-time salary adequate to attract professional mathematicians of established reputation and ability.

(C) Each department should be financed in an adequate manner.

(D) Finally, the proposed departments are not intended to duplicate the responsibilities of the central organization of the Association as carried out by the home office and the proposed Washington liaison office of the Executive Director. Nor are they intended to duplicate the work on high school text materials now being organized in an

interorganization staff of all the mathematical organizations, in which the Association may cooperate.

D. *Resolutions of thanks*

1. Whereas, the Washington Conference has been of great value to the officers and members of the Mathematical Association of America by giving an opportunity to review its past activities and to plan its future activities, and

Whereas, such a conference was made possible by a grant from the National Science Foundation, therefore

Be it resolved that those in attendance at this Conference hereby express their sincere appreciation to the Foundation for making the Conference possible.

2. This Conference votes its sincere thanks to its chairman, Professor G. Baley Price, President of the Mathematical Association of America, for having arranged the program of the Conference and for having directed its actions in such an effective manner.

Concluding Note. The resolutions were duly transmitted by the Secretary-Treasurer of the Association to the persons concerned. In particular, about 500 letters were sent in June to chairmen of departments of mathematics urging them to submit proposals to the National Science Foundation for summer institutes in 1959. A memorandum of information on N.S.F. Summer Institutes prepared by Professor E. A. Cameron was enclosed, as were announcements of two current institutes. The various resolutions on Programs of the M.A.A. and on a Plan of Action are now under consideration by the Board of Governors.

HARRY M. GEHMAN, *Secretary-Treasurer*

ON A CERTAIN FAMILY OF ARITHMETIC FUNCTIONS

PAUL J. McCARTHY, Florida State University

1. Introduction. If r is a positive integer we define the arithmetic function $T_r(n)$ in the following way: $T_r(n)$ is the number of integers k such that $1 \leqq k \leqq n$ and the greatest common divisor (k, n) is not divisible by the rth power of any prime. $T_1(n)$ is Euler's totient function $\phi(n)$ and the function $\rho(n) = T_2(n)$ was introduced and studied by Haviland in [3]. In this paper it is our purpose to investigate some of the arithmetic and asymptotic properties of the functions $T_r(n)$. The methods used are similar to those used to treat $\phi(n)$ and the results we obtain show that the $T_r(n)$ behave in a manner somewhat similar to their better-known relative.

Haviland [3] defined $T_2(n)$ in terms of the properties of certain arithmetic progressions. The other $T_r(n)$ may be defined in a similar manner. We shall say that an integer is r-free if it is not divisible by the rth power of any prime.

THEOREM 1. *$T_1(n)$ is the number of arithmetic progressions $sn+k$, $k=1, \cdots, n$, which have infinitely many prime terms. For $r \geqq 2$, $T_r(n)$ is the number of these arithmetic progressions which have infinitely many r-free terms.*

When $r=1$ this statement is an immediate consequence of Dirichlet's theo-

rem on primes in an arithmetic progression which states that if $(n, k)=1$ then $sn+k$ is a prime for infinitely many values of s ([4], pp. 73–79). In general, let $d=(n, k)$, $n=n_1d$ and $k=k_1d$. Then $sn+k=d(sn_1+k_1)$ will be r-free for infinitely many values of s if and only if d is r-free, because by Dirichlet's theorem there are infinitely many values of s for which sn_1+k_1 is a prime which does not divide d.

2. Arithmetic properties. In this section we shall show that $T_r(n)$ is a multiplicative function for each r and obtain an explicit formula for $T_r(n)$. These results will be consequences of the theorem which we prove below, in which we denote by $T_r(x, n)$ the number of integers k such that $1 \leqq k \leqq [x]$ and (n, k) is r-free. Here $[x]$ is the greatest integer $\leqq x$, and $\mu(n)$ will denote the Möbius function.

THEOREM 2.

$$T_r(x, n) = \sum_{d^r \mid n} \mu(d) \left[\frac{x}{d^r}\right].$$

We shall first prove three lemmas which are known in the case $r=1$; statements and proofs of the second and third of these lemmas in this case can be found in [5].

LEMMA 1. *If $f(n)$ is a multiplicative arithmetic function and $F(n)=\sum_{d^r \mid n} f(d)$, then $F(n)$ is multiplicative.*

For, if $(m, n)=1$,

$$\begin{aligned} F(mn) &= \sum_{d^r \mid mn} f(d) = \sum_{d_1^r \mid m, d_2^r \mid n} f(d_1 d_2) \\ &= \sum_{d_1^r \mid m, d_2^r \mid n} f(d_1) f(d_2) = \sum_{d_1^r \mid m} f(d_1) \sum_{d_2^r \mid n} f(d_2) \\ &= F(m)F(n). \end{aligned}$$

LEMMA 2. *Let $a_1, \cdots, a_s$ be any finite set of (not necessarily distinct) integers, and let $f(x)$ be a complex-valued function defined for these integers. Let S be the sum of all the $f(a_i)$ where a_i is r-free, and let S_d be the sum of all the $f(a_i)$ for which $d^r \mid a_i$. Then*

$$S = \sum \mu(d) S_d,$$

where the sum extends over all d such that d^r divides at least one a_i.

We first show that

$$\sum_{d^r \mid n} \mu(d) = \begin{cases} 1 \text{ if } n \text{ is } r\text{-free}, \\ 0 \text{ otherwise}. \end{cases}$$

Now $\mu(n)$ is a multiplicative function and so, by Lemma 1, the left-hand side of this expression is a multiplicative function of n. Therefore, it is sufficient to show that this expression is true when $n=p^a$, where p is a prime. But in this case the

left-hand side is equal to $\mu(1)=1$ if $r<a$ and to $\mu(1)+\mu(p)=0$ if $r\geqq a$.

We now have for any i,

$$f(a_i)\sum_{d^r\mid a_i}\mu(d) = \begin{cases} f(a_i) \text{ if } a_i \text{ is } r\text{-free,} \\ 0 \quad \text{otherwise.} \end{cases}$$

Hence

$$S=\sum_{i=1}^{s} f(a_i)\sum_{d^r\mid a_i}\mu(d).$$

Now choose a d whose rth power divides some a_i. Then, collecting the coefficients of $\mu(d)$, we see that we have precisely S_d. This proves the lemma.

LEMMA 3. *Let n be a positive integer and let $g(m)$ be an arithmetic function. Let $b_1, \cdots, b_s$ be positive integers. Let S be the sum of all $g(b_i)$ for which (b_i, n) is r-free, and let S_d be the sum of all $g(b_i)$ for which $d^r\mid b_i$. Then $S=\sum_{d^r\mid n}\mu(d)S_d$.*

To prove this we set $a_i=(b_i,n)$ and $f(a_i)=g(b_i)$. Then we apply Lemma 2.

Now, to prove Theorem 2 we let $b_1, \cdots, b_s$ in Lemma 3 be the integers $1, \cdots, [x]$, and we set $g(b_i)=1$ for each i. Then S is the number of integers k such that $1\leqq k\leqq [x]$ and (k, n) is r-free, *i.e.*, $S=T_r(x, n)$. Let $d^r\mid n$. Then S_d is the number of integers k such that $1\leqq k\leqq [x]$ and $d^r\mid k$, *i.e.*, the number of multiples of d^r not exceeding x. But this is just $[x/d^r]$. This proves the theorem.

COROLLARY 1. *For all n,*

$$T_r(n)=n\sum_{d^r\mid n}\frac{\mu(d)}{d^r}.$$

COROLLARY 2. *For each r, the function $T_r(n)$ is multiplicative.*

The second corollary follows from the first and from an application of Lemma 1 with $f(n)=\mu(n)/n^r$.

We can now determine $T_r(n)$ explicitly. Because of Corollary 2 we can do this by first determining $T_r(p^a)$, where p is a prime. If $a<r$ it is obvious that $T_r(p^a)=p^a$. Now suppose that $a\geqq r$. Then $T_r(p^a)$ is p^a minus the number of multiples of p^r which do not exceed p^a, *i.e.*, $T_r(p^a)=p^a-p^{a-r}$. Thus for an integer n,

$$T_r(n)=n\prod_{p^r\mid n}(1-p^{-r}).$$

3. Asymptotic properties. In this section we shall obtain some asymptotic results concerning the functions $T_r(n)$. We shall assume throughout this section that $r>1$, since the error term which we shall obtain in Theorem 3 is different from the error term which is obtained when $r=1$ (see p. 268 of [2]).

THEOREM 3. *Let $r>1$. If $T_r^*(n)=\sum_{m=1}^{n} T_r(m)$, then*

$$T_r^*(n)=\frac{n^2}{2\zeta(2r)}+O(n),$$

where $\zeta(s)$ is the Riemann zeta function.

Let $k=[n^{1/r}]$. Then

$$\begin{aligned}
T_r^*(n) &= \sum_{m=1}^{n} m \sum_{d^r\mid m} \frac{\mu(d)}{d^r} = \sum_{d^r d_1\le n} d_1\mu(d)\\
&= \sum_{d=1}^{k} \mu(d) \sum_{d_1=1}^{[n/dr]} d_1\\
&= \frac{1}{2}\sum_{d=1}^{k}\mu(d)\left\{\left[\frac{n}{d^r}\right]\left(\left[\frac{n}{d^r}\right]+1\right)\right\}\\
&= \frac{1}{2}\sum_{d=1}^{k}\mu(d)\left\{\frac{n}{d^r}+O(1)\right\}\left\{\frac{n}{d^r}+O(1)\right\}\\
&= \frac{1}{2}\sum_{d=1}^{k}\mu(d)\left\{\frac{n^2}{d^{2r}}+O\left(\frac{n}{d^r}\right)+O(1)\right\}\\
&= \frac{1}{2}n^2\sum_{d=1}^{k}\frac{\mu(d)}{d^{2r}}+O\left(\sum_{d=1}^{k}\frac{n}{d^r}\right)+O(n^{1/r}).
\end{aligned}$$

Also

$$\begin{aligned}
\frac{1}{2}n^2\sum_{d=1}^{k}\frac{\mu(d)}{d^{2r}} &= \frac{1}{2}n^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^{2r}}-\frac{1}{2}n^2\sum_{d=k+1}^{\infty}\frac{\mu(d)}{d^{2r}}\\
&= \frac{n^2}{2\zeta(2r)}+O\left(\sum_{d=k+1}^{\infty}\frac{n^2}{d^{2r}}\right),
\end{aligned}$$

where we have used the fact that ([2], p. 250)

$$\frac{1}{\zeta(s)}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^s} \qquad (s>1).$$

We complete the proof by observing that

$$\sum_{d=1}^{k}\frac{n}{d^r} \quad\text{and}\quad \sum_{d=k+1}^{\infty}\frac{n^2}{d^{2r}}$$

are both $O(n)$.

Using this theorem we can prove

THEOREM 4. *The probability that the greatest common divisor of two integers be r free is $1/\zeta(2r)$.*

Our proof follows that given by Hardy and Wright on pages 268 and 269 of [2] for the case $r=1$. Our proof will be for $r>1$. If ψ_n is the number of pairs of integers a, b such that $1 \leqq a \leqq b \leqq n$, then $\psi_n = n(n+1)/2$. But the number of these pairs whose greatest common divisor is r-free is precisely $T_r^*(n)$. Hence the probability that the greatest common divisor of a and b be r-free is

$$\lim_{n\to\infty} \frac{T_r^*(n)}{\psi_n} = \lim_{n\to\infty} \left(\frac{1}{\zeta(2r)} + \frac{O(n)}{n^2} \right) = \frac{1}{\zeta(2r)} .$$

This result, for the case $r=2$, was obtained by Christopher in [1], and a result equivalent to this, when $r=2$, is contained in Haviland's paper [3].

References

1. J. Christopher, The asymptotic density of some k-dimensional sets, this MONTHLY, vol. 63, 1956, pp. 399–401.

2. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 3rd ed., Oxford University Press, 1954.

3. E. K. Haviland, An analogue of Euler's ϕ-function, Duke Math. J., vol. 11, 1944, pp. 869–872.

4. E. Trost, Primzahlen, Birkhauser-Basel, 1953.

5. I. M. Vinogradov, Elements of Number Theory, (translated by S. Kravetz) New York, 1954.

TRANSFORMATIONS OF INTEGRALS

IAIN T. ADAMSON, The Queen's University, Belfast

The aims of this note are first, to present the theory of "change of variable" in multiple integrals in the spirit of Menger's book on the calculus [1] and second, to sketch a completely analytic treatment of a subject which is frequently dealt with by more-or-less explicit appeals to geometrical intuition. In pursuing the second aim I have been greatly helped by Ostrowski's excellent book [2].*

We begin by describing the type of "change of variable" we shall allow and the type of sets over which our integrals are taken. Let E be a set of points in real n-space, R^n. If Φ is a function of E into R^n we define the *coordinate functions* of Φ to be the real-valued functions $\phi_1, \cdots, \phi_n$ of E given by

$$\phi_i(x) = i\text{th coordinate of } \Phi(x)$$

for all points x of E. We may write $\Phi = (\phi_1, \cdots, \phi_n)$. The *Jacobian* of Φ is the real-valued function $\mathcal{J}\Phi$ of E defined by setting $\mathcal{J}\Phi(x) = \det \mathfrak{D}_j\phi_i(x)$ for all points x of E. ($\mathfrak{D}_j\phi_i$ denotes the jth first-order partial derivative of ϕ_i.) The function Φ is called a *regular transformation* of E if

* The referee has kindly drawn my attention to the book Mathematical Analysis by T. M. Apostol which also gives a completely analytic treatment of the problem discussed here without, however, mentioning orientation explicitly.

1. Φ is a (1, 1) function of E onto the image set $\Phi(E)$;

2. the coordinate functions of Φ are continuous and have continuous first-order partial derivatives at every point of E;

3. the Jacobian of Φ vanishes nowhere in E.

The following remarks are simply translations into the present terminology of standard results (see, *e.g.*, Rudin [3], Chapter 9.)

REMARK 1. *If Φ_1, Φ_2 are regular transformations of E onto E_1, E_1 onto E_2 respectively, then $\Phi = \Phi_2\Phi_1$ is a regular transformation of E onto E_2 and $\mathcal{J}\Phi = \mathcal{J}\Phi_2(\Phi_1) \cdot \mathcal{J}\Phi_1$.*

REMARK 2. *If Φ is a regular transformation of E onto E_1, then the inverse Φ^{-1} of Φ is a regular transformation of E_1 onto E.*

(In Remark 1, and throughout the paper, we adhere to Menger's convention whereby the juxtaposition fg of two functions f and g denotes the result of substituting g in f; the dot is never omitted in the symbol $f \cdot g$ for the product of the two functions.)

A function Φ of E into R^n is said to be *i-simple* if there exists a real-valued function ϕ of E such that

$$\Phi(x) = (x_1, \cdots, x_{i-1}, \phi(x), x_{i+1}, \cdots, x_n)$$

for all points $x = (x_1, \cdots, x_n)$ of E.

For each integer $n \geqq 1$ we define the *standard n-cell*, S^n, to be the set of points $(x_1, \cdots, x_n)$ in R^n which satisfy the inequalities

$$0 \leqq x_1 \leqq 1, 0 \leqq x_2 \leqq 1, \cdots, 0 \leqq x_n \leqq 1, 0 \leqq x_1 + \cdots + x_n \leqq 1.$$

A set of points E in R^n is said to be a *regular n-cell* if there exists a regular transformation of S^n onto E. The following results are easily verified.

REMARK 3. *Let E be a regular n-cell. Then E is a compact and connected set. Further, for every positive real number η there exists an interval sum* which contains all the points on the boundary of E and has volume less than η.*

From the second part of Remark 3 it follows by standard arguments that if f is a real-valued function continuous on a regular n-cell E then f is integrable over E; the value of its integral is denoted by $I(f; E)$. In particular, the function u which takes the value 1 everywhere is integrable over E; hence E has a well-defined *volume* $v(E) = I(u; E)$.

In order to give an adequate account of the effect of a "change of variable" in integrals over regular n-cells, it is essential to introduce the notion of an orientation. This idea is—informally, at least—quite familiar for regular 1-cells. The direction from left to right along the real line is conventionally called the positive direction; and so we say intuitively that a regular 1-cell is "positively oriented" if we traverse it from left to right, or if we attach to it an arrow point-

* By an interval sum we mean a finite union of closed intervals of R^n.

ing from left to right, and we say it is "negatively oriented" if we traverse it from right to left or attach to it an arrow pointing from right to left. In the same way there are familiar conventions for "orienting" regular 2-cells; we say that a 2-cell is "positively oriented" if we attach to it a counterclockwise-turning arrow and "negatively oriented" if we attach to it a clockwise-turning arrow. Now in these examples, whether we proceed by attaching an arrow to the cell E or by some other method, what we are in fact doing is attaching a sign to the cell E, or—what amounts to the same thing—we are attaching to E one of the numbers -1 or $+1$. Thus we are led to make the following definition: a *regular oriented n-cell* (E, ω) is a pair consisting of a regular n-cell E and a number ω which is either -1 or $+1$; the number ω is called the *orientation* of (E, ω). Let Φ be a regular transformation of E; then we define the image of (E, ω) under Φ to be the regular oriented n-cell $(\Phi(E), \omega_\Phi)$ where

$$\omega_\Phi = \begin{cases} +\omega & \text{if } \mathcal{J}\Phi \text{ is everywhere positive in } E, \\ -\omega & \text{if } \mathcal{J}\Phi \text{ is everywhere negative in } E. \end{cases}$$

($\mathcal{J}\Phi$ is of course of constant sign on E since E is connected and $\mathcal{J}\Phi$ is continuous and nonvanishing on E.) If f is a real-valued function continuous on E, we define the integral of f over the oriented n-cell (E, ω) to be

$$I(f; E, \omega) = I(\omega \cdot f; E).$$

We may remark in passing that the traditional notation (and Menger's) for integrals over regular 1-cells, *i.e.* over bounded closed intervals of the real line, blurs the distinction between integration over a 1-cell *simpliciter* and over an *oriented* 1-cell. The fundamental notion is that of integration *over* an interval E, but if a and b are the end-points of the interval then to write $\int_a^b f(x)dx$, or even $\int_a^b f$, and to talk of the integral *from a to b*, is to deal not with the integral over the unoriented interval E but with the integral over the oriented interval (E, ω), where $\omega = +1$ or -1 according as $a < b$ or $a > b$.

Before proceeding to our main theorem we show how a general regular transformation can be "factorized" into simple transformations.

LEMMA. *Let E be a connected set of points in R^n. Let $\Phi = (\phi_1, \cdots, \phi_n)$ be a regular transformation of E onto a set E' in R^n such that none of the first-order partial derivatives $\mathfrak{D}_1\phi_1, \cdots, \mathfrak{D}_n\phi_n$ ever vanishes in E. Then there exist a sequence of sets $E = E_0, E_1, E_2, \cdots, E_n = E'$, and a sequence of regular transformations Φ_i of E_{i-1} onto E_i $(i = 1, \cdots, n)$ such that each Φ_i is i-simple and $\Phi = \Phi_n\Phi_{n-1} \cdots \Phi_1$.*

We shall give the proof only in the case $n = 2$; the proof for the general case, which proceeds by induction, is a little more complicated.

Since $\mathfrak{D}_1\phi_1$ never vanishes in the connected set E, it follows that $\mathfrak{D}_1\phi_1$ is of constant sign in E. Let Φ_1 be the function of E onto $E_1 = \Phi_1(E)$ given by

$$\Phi_1(x, y) = (\phi_1(x, y), y)$$

for all points (x, y) of E. Then Φ_1 is certainly 1-simple; its coordinate functions are continuous and have continuous first-order partial derivatives in E; and its Jacobian vanishes nowhere in E, since clearly $\mathcal{J}\Phi_1 = \mathfrak{D}_1\phi_1$. Further, Φ_1 is a (1, 1) mapping of E onto E_1; for if $\Phi_1(x, y) = \Phi_1(x', y')$ we have at once $y = y'$ and $\phi_1(x, y) = \phi_1(x', y')$, whence $\phi_1(x, y) = \phi_1(x', y)$. Now consider the function ψ defined by setting $\psi(t) = \phi_1(t, y)$ for all appropriate real numbers t; since, by definition, $\mathfrak{D}_1\phi_1(t, y) = \mathfrak{D}\psi(t)$, it follows that $\mathfrak{D}\psi$ is of constant sign and hence that ψ is a (1, 1) function. Hence $x = x'$. This discussion shows that Φ_1 is a 1-simple regular transformation of E onto E_1.

Now set $\Phi_2 = \Phi\Phi_1^{-1}$; by Remarks 1 and 2, Φ_2 is a regular transformation of E_1 onto E'. To show that Φ_2 is 2-simple, let $(z, y) = (\phi_1(x, y), y)$ be any point of E_1; then $\Phi_2(z, y) = \Phi(x, y) = (\phi_1(x, y), \phi_2(x, y)) = (z, \phi_2(x, y))$.

This completes the proof in the case $n = 2$.

We shall use this "factorization" lemma in the proof of our central result, which we now state as follows.

THEOREM. *Let (E, ω) be a regular oriented n-cell; let Φ be a regular transformation of E onto E'. Then for every real-valued function f continuous on E' we have*

$$I(f; E', \omega_\Phi) = I(f\Phi \cdot \mathcal{J}\Phi; E, \omega). \tag{1}$$

We call (1) *the transformation rule for the situation* $(E; \Phi)$.

From this formulation of the result it is easy to deduce the two methods by which it can be applied in the practical evaluation of integrals. Reading (1) from left to right and from right to left respectively, we see that

1. to find the integral of a continuous function f over a regular n-cell E' we may try to find a regular n-cell E and a regular transformation Φ of E onto E' such that the integration of $f\Phi \cdot \mathcal{J}\Phi$ over E can be conveniently carried out;

2. to find the integral over a regular n-cell E of a function g which can be expressed in the form $g = f\Phi \cdot \mathcal{J}\Phi$, where Φ is a regular transformation of E and f is a continuous function of $\Phi(E)$, we merely integrate f over $\Phi(E)$.

We consider first the case where E and E' are bounded closed intervals of the real line and ϕ is a function of E onto E' with continuous nonvanishing derivative. The proof of (1) here is a very familiar one, slightly modified to take account of the orientation. We remark first that if F is any antiderivative of f in E', then $F\phi$ is an antiderivative of $f\phi \cdot \mathfrak{D}\phi$ in E.

Now suppose $\mathfrak{D}\phi$ is everywhere positive in E; then ϕ is an increasing function of E. Hence, if E is the interval $[a, b]$, then E' is the interval $[\phi(a), \phi(b)]$. According to the Fundamental Theorem of the Calculus, it follows that

$$I(f; E') = F(\phi(b)) - F(\phi(a)) = F\phi(b) - F\phi(a).$$

But, also by the Fundamental Theorem, we have

$$F\phi(b) - F\phi(a) = I(f\phi \cdot \mathfrak{D}\phi; E).$$

Since in the present case $\omega_\phi = \omega$, we have the desired result

$$I(f\phi \cdot \mathfrak{D}\phi;\ E,\ \omega) = I(f;\ E',\ \omega_\phi). \tag{2}$$

If, on the other hand, $\mathfrak{D}\phi$ is everywhere negative in E, then ϕ is decreasing and hence $E' = [\phi(b),\ \phi(a)]$. So in this case

$$I(f;\ E') = F\phi(a) - F\phi(b) = -I(f\phi \cdot \mathfrak{D}\phi;\ E).$$

Here, however, $\omega_\phi = -\omega$, so our final result is (2) as before.

To complete the proof of our theorem we make use of two reduction steps.

First we remark that if the transformation Φ can be carried out in two stages then it suffices to prove the theorem for each of the stages. To make this statement more explicit, let $\Phi = \Phi_2\Phi_1$, where Φ_1 is a regular transformation of E onto some regular n-cell E_1 and Φ_2 is a regular transformation of E_1 onto E'. Suppose we can prove the transformation rule for the situations $(E;\ \Phi_1)$ and $(E_1;\ \Phi_2)$. Then the rule for the situation $(E;\ \Phi)$ will follow at once by simple computations using Remark 1.

Next suppose that we can prove the transformation rule in the situation $(R;\ \Phi)$ for every regular n-cell R contained in E such that $\Phi(R)$ is a bounded closed *interval*. We claim that we can deduce the transformation rule for the situation $(E;\ \Phi)$.

To establish this result we notice first that we can certainly deduce the transformation rule for every situation $(R;\ \Phi)$ in which R is a regular n-cell contained in E and $\Phi(R) = R'$ is an interval sum. Now let S be an interval sum contained in E; let R' be an interval sum contained in E' and containing $\Phi(S)$; and let $R = \Phi^{-1}(R')$. Then

$$\begin{aligned} \left| I(f\Phi \cdot \mathfrak{J}\Phi;\ E, \omega) - I(f;\ E', \omega_\Phi) \right| \leqq{}& \left| I(f\Phi \cdot \mathfrak{J}\Phi;\ E,\ \omega) - I(f\Phi \cdot \mathfrak{J}\Phi;\ R,\ \omega) \right| \\ &+ \left| I(f;\ R',\ \omega_\Phi) - I(f;\ E',\ \omega_\Phi) \right|. \end{aligned}$$

Both terms on the right-hand side can be made arbitrarily small by choosing S and R' such that $v(E) - v(S)$ and $v(E') - v(R')$ are sufficiently small.

We now apply our lemma and the two reduction steps to show that we need prove our theorem only in the special case for which Φ is a simple transformation and $E' = \Phi(E)$ is a bounded closed interval.

To see this, let E be any regular n-cell, Φ an arbitrary regular transformation. Let x be any point of E. Since the Jacobian

$$\mathfrak{J}\Phi = \sum \pm\, \mathfrak{D}_{i_1}\phi_1 \cdot \mathfrak{D}_{i_2}\phi_2 \cdot \cdots \cdot \mathfrak{D}_{i_n}\phi_n \tag{3}$$

(where the summation runs over all permutations $(i_1, \cdots, i_n)$ of $(1, \cdots, n)$) is nonzero at x, it follows that at least one of the terms in the summation is nonzero at x. Then there exists a permutation $(i_1, \cdots, i_n)$ of $(1, \cdots, n)$ such that

$$\mathfrak{D}_{i_1}\phi_1,\ \mathfrak{D}_{i_2}\phi_2,\ \cdots,\ \mathfrak{D}_{i_n}\phi_n$$

do not vanish at x; hence there is a neighborhood of x in which they do not vanish. Applying the Heine-Borel Theorem to the covering of E provided by

the neighborhoods which correspond in this way to every point of E, we deduce easily that E can be expressed as the union of a finite number of regular n-cells E_k, having only boundary points in common and such that for every k there exists a permutation of $(1, \cdots, n)$ for which the corresponding term in the summation (3) is nonvanishing on E_k. For each E_k it follows then by a suitable modification of the indexing in our lemma that there exist sequences of regular n-cells

$$E_k = E_{k,0}, E_{k,1}, E_{k,2}, \cdots, E_{k,n} = \Phi(E_k)$$

and of *simple* regular transformations $\Phi_{k,r}$ of $E_{k,r-1}$ onto $E_{k,r}$ such that $\Phi_{k,n}\Phi_{k,n-1}\cdots\Phi_{k,1}$ is the restriction of Φ to E_k.

If now we can prove our transformation rule in every situation $(R; \Phi_{k,r})$ where R is a subset of $E_{k,r-1}$ for which $\Phi_{k,r}(R)$ is a bounded closed interval, then, from our second reduction step the transformation rule for every situation $(E_{k,r-1}; \Phi_{k,r})$ follows at once. Using the first reduction step we can deduce the rule for every situation $(E_k; \Phi)$, and so finally, by addition, for the situation $(E; \Phi)$.

We conclude the proof of our theorem, then, by proving the transformation rule for a situation $(E; \Phi)$ where $E' = \Phi(E)$ is a bounded closed interval of R^n and Φ is a simple transformation. Suppose, then, that E' is defined by the inequalities $a_i \leqq x_i \leqq b_i$ $(i = 1, \cdots, n)$ and that Φ is n-simple, *i.e.* that there exists a real-valued function ϕ of E such that $\Phi(x) = (x_1, \cdots, x_{n-1}, \phi(x))$ for all points $x = (x_1, \cdots, x_n)$ of E.

Let $\overline{E}$ be the bounded closed interval of R^{n-1} defined by the inequalities $a_i \leqq y_i \leqq b_i$ $(i = 1, \cdots, n-1)$. For every point $y = (y_1, \cdots, y_{n-1})$ of $\overline{E}$ consider the set of real numbers t such that $(y, t) = (y_1, \cdots, y_{n-1}, t)$ belongs to E; these points t form an interval E_y of the real line such that $\phi(y, E_y) = [a_n, b_n]$.

Let ϕ_y be the function of E_y onto $[a_n, b_n]$ defined by setting $\phi_y(t) = \phi(y, t)$. Then $\mathfrak{D}\phi_y(t) = \mathfrak{D}_n\phi(y, t) = \mathfrak{J}\Phi(y, t)$; hence $\mathfrak{D}\phi_y$ is continuous and of constant sign in E_y. It follows from the special case of our theorem for intervals of the real line that for every real-valued function f continuous on E we have

$$I(f_y\phi_y \cdot \mathfrak{D}\phi_y; E_y, \omega) = I(f_y; [a_n, b_n], \omega_\Phi), \tag{4}$$

where f_y is defined in the same way as ϕ_y above.

Now define the functions F and G of $\overline{E}$ by setting for every point y of $\overline{E}$

$$F(y) = \text{left-hand side of (4)}, \quad G(y) = \text{right-hand side of (4)}.$$

Since it is easily seen that $f_y\phi_y \cdot \mathfrak{D}\phi_y = (f\Phi \cdot \mathfrak{J}\Phi)_y$, it follows from standard results on the reduction of multiple integrals to repeated integrals that

$$I(F; \overline{E}) = I(f\Phi \cdot \mathfrak{J}\Phi; E, \omega).$$

Similarly we have $I(G; \overline{E}) = I(f; E', \omega_\Phi)$. Since, by (4), $F = G$, our desired result follows and our theorem is completely proved.

We remark that many of the situations $(E; \Phi)$ with which we have to deal in the practical evaluation of multiple integrals do not satisfy the condition that Φ is regular on E. We may mention as an example the polar-coordinate transformation Π in the real plane given by

$$\Pi(r, \theta) = (r \cos \theta, r \sin \theta),$$

which is not regular in any regular 2-cell including the origin. Only slight modifications are necessary to deal with situations, such as that of the example, in which the lack of regularity is not too unpleasant. If E is a regular n-cell in R^n, we say that a function Φ of E onto a regular n-cell E' in R^n is *almost regular* if for every positive real number η there exists a regular n-cell E_η contained in E such that Φ is a regular transformation of E_η and such that $v(E)-v(E_\eta)$ and $v(E')-v(\Phi(E_\eta))$ are both less than η. It is then a simple matter to prove the following result.

THEOREM. *Let (E, ω) be a regular oriented n-cell; let Φ be an almost regular transformation of E onto a regular n-cell E'. Then for every real-valued function f continuous on E' we have*

$$I(f; E', \omega_\Phi) = I(f\Phi \cdot \mathfrak{J}\Phi; E, \omega).$$

References

1. K. Menger, Calculus, a Modern Approach, Boston, 1955.
2. A. Ostrowski, Vorlesungen über Differential- und Integralrechnung, Band III, Basel, 1954.
3. W. Rudin, Principles of Mathematical Analysis, New York, 1953.

GROUPOIDS WITH ADDITIVE ENDOMORPHISMS

I. M. H. ETHERINGTON, University of Edinburgh

The main purpose of this note is to prove two results (Theorems 1(ii) and 3) concerning the logarithmetic [3, 6, 7] of a groupoid with additive endomorphisms. These results apply in particular to groupoids with the property $xy \cdot zw = xz \cdot yw$, since these have additive endomorphisms [8]. Theorem 1 as applied to quasigroups with this property was given by Murdoch [10]. Theorem 4 states a general result on logarithmetics, and Theorem 5 a condition under which a logarithmetic has, with respect to addition, additive endomorphisms.

1. Endomorphisms of groupoids. Let G be a groupoid, *i.e.*, a set of elements closed with respect to a binary operation, which I shall write as multiplication. If

$$\alpha: x \to x^\alpha$$

is a mapping of G into itself, and β also is such a mapping, we define the mappings $\alpha+\beta$, $\alpha\beta$ by the rules

$$x^{\alpha+\beta} = x^\alpha x^\beta, \qquad x^{\alpha\beta} = (x^\alpha)^\beta.$$

This addition is in general nonassociative, like the multiplication in G, but the multiplication of mappings is associative.

If γ also is such a mapping, then of the two distributive laws

$$\gamma(\alpha+\beta) = \gamma\alpha + \gamma\beta, \qquad (\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$$

the first is always valid, for we have

$$x^{\gamma(\alpha+\beta)} = x^{\gamma\alpha}x^{\gamma\beta} = x^{\gamma\alpha+\gamma\beta} \qquad \text{(all } x \text{ of } G\text{)}.$$

If γ is an endomorphism of G, *i.e.* such that $(xy)^\gamma = x^\gamma y^\gamma$ for all x, y of G, then the second distributive law also holds, for

$$x^{(\alpha+\beta)\gamma} = (x^\alpha x^\beta)^\gamma = x^{\alpha\gamma}x^{\beta\gamma} = x^{\alpha\gamma+\beta\gamma} \qquad \text{(all } x \text{ of } G\text{)}.$$

The set E_G of endomorphisms of G, together with the operation of multiplication of endomorphisms, forms the endomorphism semigroup $E^\times(G)$. If G has the property that the sum of two endomorphisms is always an endomorphism, we shall say that G has *additive endomorphisms*. In this case E_G with addition forms an additive groupoid $E^+(G)$, while E_G with both operations forms the endomorphism ringoid $E(G)$, in which the associative law of multiplication and both distributive laws hold.

If a groupoid has a set of generators $a, b, \cdots$ (as every finite groupoid must have), then an endomorphism α is fully determined when we know the images of the generators; for every element x can be expressed as a finite "word" in the generators, whence we can calculate its image x^α. In other words, any mapping of the generators onto elements of G can be extended in at most one way to an endomorphism of G.

A groupoid with one generator will be called *cyclic*.

2. Entropic groupoids. By the *entropic* law of multiplication I mean the identity*

$$xy \cdot zw = xz \cdot yw. \tag{1}$$

The word *entropic*, introduced in [5], refers by etymology to "inner turning" and seems preferable to *symmetric* which was used with the same meaning by Frink in a recent note† [8]. An objection to use of the word *symmetric* is that this conflicts with its established meaning when applied to groups and semigroups; also that *totally symmetric* has been used by Bruck [2] very appropriately for the property that $xy=z$ implies the five other equations derived by permuting x, y, z. This was in the context of quasigroups, and Bruck followed Murdoch [10, 11] in calling entropic quasigroups *abelian* on account of analogies with abelian groups. Unfortunately *abelian* has also been used by some writers

* The generalization for n-ary operations [5] is $\prod_i \prod_j x_{ij} = \prod_j \prod_i x_{ij}$ $(i, j = 1, \cdots, n)$.

† Frink uses the additive notation for groupoids and the opposite order for products of endomorphisms.

on quasigroups [*e.g.* **9**] to mean commutative. I propose to use *entropic* for all groupoids having the property (1). (Stein [**12**] uses the term *medial*.)

Frink observes that an entropic groupoid G has additive endomorphisms. For if α, β are endomorphisms, we have, using the entropic property,

$$(xy)^{\alpha+\beta} = (xy)^{\alpha}(xy)^{\beta} = x^{\alpha}y^{\alpha} \cdot x^{\beta}y^{\beta} = x^{\alpha}x^{\beta} \cdot y^{\alpha}y^{\beta} = x^{\alpha+\beta}y^{\alpha+\beta},$$

so that $\alpha+\beta$ is an endomorphism. But Frink goes further and [**8**, pp. 700, 701, 703] implies, almost says, that the converse is true, that the sum of two endomorphisms is always an endomorphism *only* if G is entropic. This is not so. I give below the multiplication tables of three groupoids, having respectively 2, 6 and 7 elements, which all have additive endomorphisms but are *not* entropic.

(2) Ex. 1. $G = \{a, b\}$. $a^2 = b^2 = ab = b$, $ba = a$.

Ex. 2. $G = \{a, b, c, d, e, f\}$.

All products involving e or $f = f$.

	a	b	c	d
a	b	c	d	e
b	c	d	e	f
c	d	f	f	f
d	e	f	f	f

Ex. 3. $G = \{a, b, c, d, e, f, g\}$.

All products involving e, f or $g = g$.

	a	b	c	d
a	b	d	g	g
b	c	g	e	g
c	g	g	g	g
d	g	f	g	g

These groupoids are not entropic because in each case $aa \cdot ba \neq ab \cdot aa$. They are cyclic, the element a being in case the generator. It is readily verified that Example 1 has two endomorphisms, each determined by a mapping of a:

$$\alpha\colon a \to a,\ b \to b, \qquad \beta\colon a \to b,\ b \to b,$$

with the closed addition table, isomorphic to (2):

$$\alpha + \alpha = \beta + \beta = \alpha + \beta = \beta, \qquad \beta + \alpha = \alpha.$$

Similar results will be found for Examples 2 and 3; in each case $E^+(G) \simeq G$ $(+ \to \times)$.

(Example 2 is derived from an example in [**7**, p. 158]. Example 3 was communicated to me by Mr. H. Minc.)

3. Logarithmetics. Let powers of elements of G be indicated by indices, beginning with $x^1 = x$, $x^2 = xx$, and let addition and multiplication of indices be defined as for mappings:

$$x^{A+B} = x^A x^B, \qquad x^{AB} = (x^A)^B.$$

Thus for example

$$x^{2+1} = x^2x, \qquad x^{(1+2)2} = (xx^2)^2, \qquad x^{2(1+2)} = x^2(x^2)^2 = x^{2+2.2}. \tag{3}$$

Given the groupoid G, we equate two indices, $A = B$, if $x^A = x^B$ for all x of G. The *logarithmetic* $L(G)$ then consists of the classes of equated indices, with the operations $+$ and $\times$. A class of equated indices will be called an *index number*, or *index* for short. Just as with additive endomorphisms, we can also consider $L^+(G)$ and $L^\times(G)$ separately, each having the indicated operation.*

In general, addition of indices is nonassociative, but multiplication is associative, and the first distributive law

$$A(B + C) = AB + AC \tag{4}$$

holds, as illustrated in (3). Further identities will hold in particular logarithmetics; for example, G is *palintropic* [4] if $x^{AB} = x^{BA}$ for all x of G and all indices A, B, so that

$$AB = BA \tag{5}$$

in $L(G)$, and then the second distributive law holds:

$$(B + C)A = BA + CA. \tag{6}$$

Conversely, (6) implies (5) [5, Theorem 3]. G is *power entropic* if $L^+(G)$ is entropic, *i.e.* if indices satisfy $(A+B)+(C+D) = (A+C)+(B+D)$; this implies, but is not implied by, the palintropic property of G [5, 7]. G may be called *trivially palintropic* if all products of six elements are the same. For this implies validity of

$$x^{(1+2)2} = x^{2(1+2)}, \qquad x^{(2+1)2} = x^{2(2+1)},$$

and of all more complicated cases of $x^{AB} = x^{BA}$, while the simpler cases where A and B are 1 or 2 hold automatically. The groupoids of Examples 1, 2, 3 are trivially palintropic but not power entropic.

4. We shall use what may be called *nonassociative induction*: If a (multiplicative) groupoid G has generators $a, b, \cdots$, then in order to prove a theorem Θ_x for all x of G, it is enough to verify $\Theta_a, \Theta_b, \cdots$ and to prove that Θ_x, Θ_y together imply Θ_{xy} for all x, y of G.

THEOREM 1. *If a groupoid G has additive endomorphisms, then* (i) *powers are endomorphisms of G,* (ii) *G is palintropic.*

* In speaking of a *power* x^A we shall have in mind the corresponding mapping $x \to x^A$ of G into itself. Thus two powers which effect the same mapping are identified. The set of such mappings with the operation $+$ forms the free algebra $F_1(G)$ [1, p. viii]. $L^+(G)$ is isomorphic to $F_1(G)$, of which it is an abstract model. $F_1(G)$ consists of mappings of G, while $L^+(G)$ consists of classes of indices; hence two different groupoids may have the *same* logarithmetic when it can only be said that their F_1's are isomorphic. If further operations besides multiplication are defined in G, the logarithmetic remains as defined while the free algebra becomes more complicated: see [7] for further remarks in this connection.

(i) means that if P is any index $(xy)^P = x^P y^P$. The proof is by nonassociative induction on the index. Indices form a cyclic additive groupoid with generator 1. The result is obvious when $P=1$; and if two powers $x \to x^A$, $x \to x^B$ are endomorphisms of G, then so is the power $x \to x^{A+B}$, since this is the sum of two endomorphisms. This proves (i).

It follows that the indices of powers obey the second distributive law (6), because endomorphisms obey it. This is equivalent to the palintropic property (5). (The proof of this equivalence given in [5] was again by nonassociative induction.)

I do not suppose that the converse of (i) holds. Consideration of nonabelian groups shows that the converse of (ii) is false.

THEOREM 2. *If G is a cyclic groupoid with generator a, then its additive logarithmetic $L^+(G)$ is homomorphic to G, addition corresponding to multiplication and 1 corresponding to a.*

For any element x of G is expressible as a power of the generator, $x = a^P$, not necessarily with uniquely determined index number. Thus the correspondence $P \to a^P$ maps $L^+(G)$ on all G, with $1 \to a$. It is a homomorphism because

$$P + Q \to a^{P+Q} = a^P a^Q,$$

i.e., the image of the sum of two indices is the product of their images.

THEOREM 3. *If G is a cyclic groupoid with additive endomorphisms, then its logarithmetic $L(G)$ and endomorphism ringoid $E(G)$ are isomorphic, and additively are isomorphic to G.*

For any mapping of the generator onto an element of G, say $a \to a' = a^P$, extends in *at most* one way to an endomorphism of G (see Section 1), and in *at least* one way to a power $x \to x^P$, and hence by Theorem 1(i) in one and only one way to each, powers and endomorphisms coinciding. $L(G) \simeq E(G)$ follows. The fact that a mapping of a extends in only one way to a power means that each possible image a' is expressible in only one way as a power a^P. The correspondence in Theorem 2 is therefore an isomorphism. Thus $L^+(G) \simeq E^+(G) \simeq G$ with $+ \to + \to \times$.

Example. For the cyclic group C_n, L and E are both isomorphic to the ring of residues mod n.

THEOREM 4. *For any groupoid G, $L^\times(G)$ is anti-isomorphic to the endomorphism semigroup of $L^+(G)$.*

Proof. Any fixed index number A determines the mapping

$$\alpha_A : P \to AP \tag{7}$$

of $L^+(G)$ into itself, in which $1 \to A$. The distributive law (4) shows that α_A is an endomorphism of $L^+(G)$. Since $L^+(G)$ is cyclic, this is the unique endomorphism in which the generator 1 is mapped on A; hence all endomorphisms of $L^+(G)$

are accounted for thus. The correspondence $A \leftrightarrow \alpha_A$ is therefore one-one both ways between $L^{\times}(G)$ and $E^{\times}L^{+}(G)$; and it is an anti-isomorphism because $\alpha_A\alpha_B$ is the mapping $P \rightarrow BAP$, *i.e.*, α_{BA}.

THEOREM 5. *If G is palintropic, $L^{+}(G)$ has additive endomorphisms.*

For the endomorphisms of $L^{+}(G)$ are of the form (7), and by (6) $\alpha_A+\alpha_B$ is the mapping $P \rightarrow AP + BP = (A + B)P$, which is the endomorphism α_{A+B}. (From Theorems 1 and 5, if G has additive endomorphisms, so has $L^{+}(G)$.)

References

1. G. Birkhoff, Lattice Theory, rev. ed., Amer. Math. Soc. Colloquium Publications, vol. 25, New York, 1948.

2. R. H. Bruck, Some results in the theory of quasigroups, Trans. Amer. Math. Soc., vol. 55, 1944, pp. 19–52.

3. I. M. H. Etherington, Some non-associative algebras in which the multiplication of indices is commutative, J. London Math. Soc., vol. 16, 1941, pp. 48–55.

4. ———, Transposed algebras, Proc. Edinburgh Math. Soc. (2), vol. 7, 1945, pp. 104–121.

5. ———, Non-associative arithmetics, Proc. Roy. Soc. Edinburgh (A), vol. 62, 1949, pp. 442–453.

6. ———, Non-commutative train algebras of ranks 2 and 3, Proc. London Math. Soc. (2), vol. 52, 1951, pp. 241–252.

7. ———, Theory of indices for non-associative algebra, Proc. Roy. Soc. Edinburgh (A), vol. 64, 1955, pp. 150–160.

8. O. Frink, Symmetric and self-distributive systems, this MONTHLY, vol. 62, 1955, pp. 697–707.

9. Harriet Griffin, The abelian quasi-group, Amer. J. Math., vol. 62, 1940, pp. 725–737.

10. D. C. Murdoch, Quasi-groups which satisfy certain generalized associative laws, Amer. J. Math., vol. 61, 1939, pp. 509–522.

11. ———, Structure of abelian quasigroups, Trans. Amer. Math. Soc., vol. 49, 1941, pp. 392–409.

12. S. K. Stein, On the foundations of quasigroups, Trans. Amer. Math. Soc., vol. 85, 1957, pp. 228–256.

THE CONCURRENCY OF PERPENDICULARS

PAUL A. CLEMENT, State College of Washington

Introduction. In the determination of possible concurrency of cevians of a triangle, Ceva's theorem ([1] p. 50) plays an important and useful role. We establish here a theorem which is a kind of "companion" to Ceva's in that it plays a similar role in the determination of concurrency of perpendiculars to the sides of a triangle.

Definitions. The symbol (K, L, M) will indicate three points K, L, and M, on the sides (possibly produced) BC, CA and AB respectively of a triangle ABC. We consider directed segments with $\overline{AM} = -\overline{MA}$, so that for example $\overline{AM}+\overline{MB} = \overline{AB}$ for all positions of M on the line $\overline{AB}$.

The points (K, L, M) will be said to satisfy condition C if the cevians AK, BL, and CM are concurrent, and then the point of concurrency will be called the C-point of (K, L, M).

The points (K, L, M) will be said to satisfy condition P if the perpendiculars to the sides of the triangle erected at K, L, and M are concurrent, and then the point of concurrency will be called the P-point of (K, L, M).

Thus, if A', B', and C' are the midpoints of the sides opposite A, B, and C, (A', B', C') satisfy condition C, and the C-point here is the centroid of the triangle. We note that the orthocenter is both a C-point and P-point.

The "Companion" Theorem. Ceva's theorem and its converse may now be stated in the following way: The points (K, L, M) satisfy condition C if and only if $\overline{AM}\cdot\overline{BK}\cdot\overline{CL}=\overline{MB}\cdot\overline{KC}\cdot\overline{LA}$. We shall prove the following

THEOREM. *The points (K, L, M) satisfy condition P if and only if*

$$\overline{AM}^2+\overline{BK}^2+\overline{CL}^2=\overline{MB}^2+\overline{KC}^2+\overline{LA}^2. \tag{1}$$

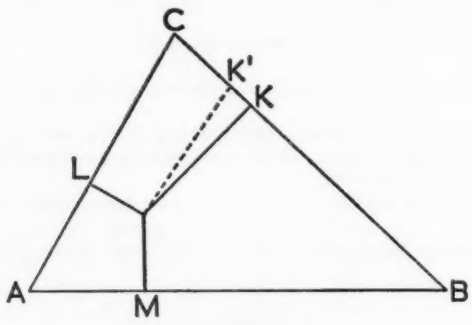


FIG. 1

Proof. (*Necessity*). From P (see Fig. 1) drop perpendiculars to the sides and join P to A and B. In right triangles PAM and PBM we have that

$$\overline{AM}^2=\overline{AP}^2-\overline{PM}^2, \text{ and } \overline{MB}^2=\overline{BP}^2-\overline{PM}^2.$$

By subtraction, we get that

$$\overline{AM}^2-\overline{MB}^2=\overline{AP}^2-\overline{BP}^2. \tag{2c}$$

Similar relations, (2a) and (2b), are obtained in the triangles BCP and CAP, and the addition of these three, (2a), (2b), and (2c), results in (1).

(*Sufficiency*). Suppose (1) to hold, that perpendiculars at M and L intersect at P, and that the perpendicular from P to BC intersects at K'. Then, by the necessity proof, we have that

(3) $$\overline{AM}^2 + \overline{BK'}^2 + \overline{CL}^2 = \overline{MB}^2 + \overline{K'C}^2 + \overline{LA}^2.$$

Now subtract (3) from (1) to get that

$$\overline{BK}^2 - \overline{BK'}^2 = \overline{KC}^2 - \overline{K'C}^2, \text{ or } \overline{BK}^2 - \overline{KC}^2 = \overline{BK'}^2 - \overline{K'C}^2;$$

and it is easily seen that this holds only if $K = K'$.

COROLLARY. *Each of the following four relations is equivalent to* (1), *(a, b, and c denote the length of the sides opposite A, B, and C).*

(4) $$c\cdot\overline{AM} + a\cdot\overline{BK} + b\cdot\overline{CL} = c\cdot\overline{MB} + a\cdot\overline{KC} + b\cdot\overline{LA},$$

(5) $$2(c\cdot\overline{AM} + a\cdot\overline{BK} + b\cdot\overline{CL}) = c^2 + a^2 + b^2,$$

(6) $$\overline{AM}\cdot\sin C + \overline{BK}\cdot\sin A + \overline{CL}\cdot\sin B = \overline{MB}\cdot\sin C + \overline{KC}\cdot\sin A + \overline{LA}\cdot\sin B,$$

and

(7) $$\pm c\cdot\overline{MM_1} \pm a\cdot\overline{KK_1} \pm b\cdot\overline{LL_1} = 0,$$

where (K_1, L_1, M_1) are the isotomic points of (K, L, M) and (7) *holds for some choice of signs.*

Proof. We obtain (4) by transposing in (1) and factoring pairs; (5) comes from (4) when an expression equal to the left member of (4) is added to both sides of (4); the Sine Law substituted in (4) produces (5); (7) is obtained by transposing in (4) and identifying segments.

We remark that (4) seems to be the most useful in this set of equivalent relations. Using (4), one easily deduces the concurrency of the altitudes, the perpendicular bisectors of the sides, *etc.*

COROLLARY. *If (K, L, M) satisfy condition P, then so also do (K_1, L_1, M_1), where K_1, L_1, and M_1 are the isotomic points of K, L, and M.*

Proof. This is obvious either from (7) or (4). Two P-points related as in this corollary will be called *isotomic mates* (cf. isotomic conjugate points ([1] p. 169). Thus, perpendiculars erected at the "internal" touch points of the excircles of a triangle are concurrent, and the corresponding P-point is the isotomic mate of I, the incenter of the triangle.

Points on the Circumcircle. We may now conveniently restate two theorems ([1] p. 152) on the Simson line.

THEOREM. *The points (K, L, M) determine a point on the circumcircle of the triangle ABC (which is their P-point) if and only if both (K, L, M) satisfy condition P and (K, L, M) are collinear.*

Proof. See reference given; however, it is an interesting exercise to prove this theorem using segment lengths in (4) and in $\overline{AM}\cdot\overline{BK}\cdot\overline{CL} = (-1)\ \overline{MB}\cdot\overline{KC}\cdot\overline{LA}$, the latter being a necessary and sufficient condition that (K, L, M) be collinear.

A Property of the Nine-Point Circle. The following theorem generalizes a property of the nine-point circle and also presents a kind of converse to another theorem ([1] p. 170, prob. 9).

THEOREM. *Let* (K, L, M) *be noncollinear and satisfying condition* P. *Then the circumscribing circle of* (K, L, M) *intersects the sides of the triangle* ABC *in* (K', L', M') *which also satisfy condition* P; *further, the corresponding* P*-points,* P *and* P', *are isogonal conjugates and* R, *the center of the circle, is the midpoint of* $\overline{PP'}$.

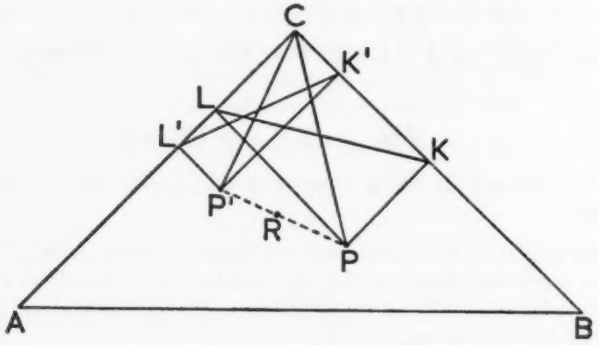


FIG. 2

Proof. The circle circumscribing (K, L, M) intersects the sides of the triangle (Fig. 2) with chords $\overline{KK'}$, $\overline{LL'}$, and $\overline{MM'}$; let K_1, L_1, and M_1 be the midpoints of these chords. Obviously (K_1, L_1, M_1) satisfy condition P, the P-point being R, the center of the circle. Thus, we have that

$$c\cdot A\overline{M} + a\cdot\overline{BK} + b\cdot\overline{CL} = c\cdot\overline{MB} + a\cdot\overline{KC} + b\cdot\overline{LA}, \tag{8}$$

and

$$c\cdot A\overline{M}_1 + a\cdot\overline{BK}_1 + b\cdot\overline{CL}_1 = c\cdot\overline{M}_1\overline{B} + a\cdot\overline{K}_1\overline{C} + b\cdot\overline{L}_1\overline{A}. \tag{9}$$

Subtract (8) from (9) to get that

$$c\cdot\overline{MM}_1 + a\cdot\overline{KK}_1 + b\cdot\overline{LL}_1 = c\cdot\overline{M}_1\overline{M} + a\cdot\overline{K}_1\overline{K} + b\cdot\overline{L}_1\overline{L};$$

and since (K_1, L_1, M_1) are midpoints, it follows that

$$c\cdot\overline{M}_1\overline{M}' + a\cdot\overline{K}_1\overline{K}' + b\cdot\overline{L}_1\overline{L}' = c\cdot\overline{M}'\overline{M}_1 + a\cdot\overline{K}'\overline{K}_1 + b\cdot\overline{L}'\overline{L}_1. \tag{10}$$

On adding (9) and (10), we find that

$$c\cdot\overline{AM}' + a\cdot\overline{BK}' + b\cdot\overline{CL}' = c\cdot\overline{M}'\overline{B} + a\cdot\overline{K}'\overline{C} + b\cdot\overline{L}'\overline{A},$$

which is the condition that (K', L', M') satisfy condition P. It is obvious that

R is the midpoint of $\overline{PP'}$. Finally,

$$\begin{aligned}\angle L'CP' + \angle P'CP &= \angle LKP, \text{ since } CLPK \text{ is inscribable,}\\ &= 90° - \angle K'KL\\ &= 90° - \angle LL'K', \text{ since } KK'LL' \text{ is inscribable,}\\ &= \angle K'L'P'\\ &= \angle KCP + \angle P'CP, \text{ since } CL'P'K' \text{ is inscribable.}\end{aligned}$$

Thus $\angle L'CP' = \angle KCP$, and similarly at the other vertices, so that P and P' are isogonal conjugates.

It is evident that our circumscribing circle is the nine-point circle of the triangle ABC if (K, L, M) are the midpoints of the sides, in which case P and P' become 0, the circumcenter, and H, the orthocenter, respectively.

Reference

1. D. R. Davis, Modern College Geometry, 1949.

MATHEMATICAL NOTES

EDITED BY ROY DUBISCH, Fresno State College

Material for this department should be sent to Roy Dubisch, Department of Mathematics, Fresno State College, Fresno 26, California.

NOTES ON MATRIX THEORY—XIV: ON THE JACOBI RELATION FOR THE BRACKET SYMBOL

RICHARD BELLMAN, The RAND Corporation

1. Introduction. Let $[A, B]$ denote the commutator expression $AB - BA$ where A and B are square matrices. The object of this note is to derive, rather than verify, the classical three-term relation

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0. \tag{1}$$

2. Preliminaries. Let e^A denote the matrix exponential, and write

$$e^A e^B = e^{A+B+f(A,B)}, \tag{1}$$

where

$$f(A, B) = [A, B]/2 + g(A, B) + h(A, B), \tag{2}$$

where $g(A, B)$ is a homogeneous polynomial of degree 3 in A and B satisfying the relation

$$g(A, B) = g(B, A), \tag{3}$$

and $h(A, B)$ is a sum of homogeneous polynomials in A and B beginning with one of degree 4.

3. Associativity. Let us now employ the associative property of matrices. We have

$$e^A(e^Be^C) = (e^Ae^B)e^C. \tag{1}$$

Hence

$$e^Ae^{B+C+f(B,C)} = e^{A+B+f(A,B)}e^C. \tag{2}$$

Using (2.1) again, this yields the basic functional equation

$$f(B, C) + f(A, B + C + f(B, C)) = f(A, B) + f(A + B + f(A, B), C). \tag{3}$$

4. Derivation of Jacobi relation. Let us now use the relation of (2.2) in (3.3) We obtain

$$\begin{aligned} &f(B, C) + f(A, B + C + f(B, C)) \\ &\quad = [B, C]/2 + g(B, C) + 1/2[A, B + C + [B, C]/2] \\ &\qquad + g(A, B + C) + \text{terms of degree four or more.} \end{aligned} \tag{1}$$

Hence to terms of degree four,

$$\begin{aligned} &f(B, C) + f(A, B + C + f(B, C)) \\ &\quad = [B, C]/2 + [A, B + C]/2 + [A, [B, C]]/4 + g(B, C) + g(A, B + C), \\ &f(A, B) + f(A + B + f(A, B), C) \\ &\quad = [A, B]/2 + [A + B, C]/2 + [[A, B], C]/4 + g(A, B) + g(A + B, C). \end{aligned} \tag{2}$$

Using the linearity of the bracket symbol, $[X+Y, Z]=[X, Z]+[Y, Z]$, this relation reduces to

$$\begin{aligned} &\frac{[A, [B, C]]}{4} + g(B, C) + g(A, B + C) \\ &\qquad = \frac{[[A, B], C]}{4} + g(A, B) + g(A + B, C). \end{aligned} \tag{3}$$

Let us now permute the symbols cyclically, replacing A by B, B by C, C by A, and then A by C, B by A, C by B, and then add.

Cancelling the common terms, we obtain

$$\begin{aligned} &(1/4)\{[A, [B, C]] + [B, [C, A]] + [C, [A, B]]\} \\ &\qquad + \{g(A, B + C) + g(B, C + A) + g(C, A + B)\} \\ &\quad = (1/4)\{[[A, B], C] + [[B, C], A] + [[C, A], B]\} \\ &\qquad + \{g(A + B, C) + g(B + C, A) + g(C + A, B)\}. \end{aligned} \tag{4}$$

Referring to (1.3), we see that the g-terms cancel. Using the result that $[A, B] = -[B, A]$, we obtain (1.1).

A TEMPERATURE FUNCTION WHICH VANISHES INITIALLY

P. C. ROSENBLOOM, University of Minnesota and D. V. WIDDER, Harvard University

In the theory of heat conduction it is well known that the temperature of an infinite bar is not uniquely determined by its temperature at any given instant. The function

$$u(x, t) = xt^{-3/2}e^{-x^2/4t}$$

satisfies the heat equation

$$\frac{\partial^2 u}{\partial x^2} = \frac{\partial u}{\partial t} \tag{1}$$

for $t>0$, and $u(x, 0+)=0$ for $-\infty<x<\infty$. This example, usually cited to substantiate the failure of uniqueness, is unsatisfactory for some purposes since it is discontinuous at the origin. The purpose of the present note is to exhibit a solution of equation (1) which is of class C^∞ over the whole plane, vanishes for $t=0$, but which is not identically zero. Various other authors, including E. Hille [1], L. Hörmander [2], S. Täcklind [3], and A. Tychonov [4], have shown the existence of such solutions. The advantage of the present example is that it can be set down explicitly and that its properties can be derived in a very elementary way.

Set

$$g(x, t) = e^x \cos(x + 2t) + e^{-x} \cos(x - 2t),$$
$$a(y) = e^{-y^{4/3}} y \cos(\sqrt{3}y^{4/3}).$$

The required function is

$$u(x, t) = \int_0^\infty a(y)g(xy, ty^2)dy. \tag{2}$$

It is clear that $g(xy, ty^2)$ satisfies (1) over the whole plane for each value of the parameter y. It will be evident that $u(x, t)$ satisfies (1) and is of class C^∞ if differentiation under the integral sign is valid. But

$$\left|\frac{\partial^{2n} g(x, t)}{\partial x^{2n}}\right| = \left|\frac{\partial^n g(x, t)}{\partial t^n}\right| \leqq 2^{n+1} \cosh x. \tag{3}$$

Now differentiate the integral (2) n times with respect to t or $2n$ times with respect to x under the integral sign. The step will be valid if the resulting integral is dominated, say for $|x| \leqq R$, $-\infty<t<\infty$, by another convergent one in which the integrand is independent of x and t. But (3) gives the dominant integral

$$2^{n+1}\int_0^\infty e^{-y^{4/3}} y^{2n+1} \cosh Ry \, dy,$$

obviously convergent for every $R>0$.

We now show that

$$u(x, 0) = 2\int_0^\infty a(y)\cosh xy\cos xy\,dy = 0, \qquad -\infty < x < \infty. \tag{4}$$

By adding the four series

$$e^{\pm xy\pm ixy} = \sum_0^\infty (\pm 1 \pm i)^n \frac{(xy)^n}{n!} \ll \sum_0^\infty \frac{2^n|xy|^n}{n!},$$

we have

$$\cosh xy\cos xy = \sum_0^\infty \frac{a_n(xy)^{4n}}{4n!} \ll \sum_0^\infty \frac{2^n|xy|^n}{n!} \tag{5}$$

for suitable, but irrelevant, constants a_n. Now substitute the series (5) in the integral (4) and integrate term by term, a valid step since

$$\int_0^\infty e^{-y^{4/3}}ye^{2|xy|}dy < \infty, \qquad -\infty < x < \infty.$$

But now (4) is established since it is well known that

$$\int_0^\infty a(y)y^{4n}dy = 0, \qquad n = 0, 1, 2, \cdots. \tag{6}$$

For completeness we add the proof. The integral (6) is the real part of

$$\int_0^\infty e^{-y^{4/3}z}y^{4n+1}dy = (3/4)\,\Gamma[3(2n+1)/2]z^{-3(2n+1)/2}, \tag{7}$$

where $z = 1 - i\sqrt{3}$. But

$$\arg z^{-3(2n+1)/2} = \frac{3(2n+1)}{2}\cdot\frac{\pi}{3} = (2n+1)\frac{\pi}{2}.$$

That is, the integral (7) is purely imaginary, and (6) is established. Finally,

$$u(0, t) = 2\int_0^\infty a(y)\cos 2ty^2dy \tag{8}$$

is not identically zero by the uniqueness theorem for Fourier-cosine transforms of functions in the class L. We observe that $a(y)$ might be replaced by many others which are known to make the moments (6) all vanish.

From the general theory of Hörmander [2] one could also exhibit the closely-related solution

$$u(x, t) = \int_{a-i\infty}^{a+i\infty} e^{st+x\sqrt{s}-s^{3/2}}ds, \qquad a > 0,$$

where the integration is along the line Re $s=a$ of the complex s-plane. This solution has the additional feature that it vanishes identically for negative t. Equation (8) shows that this is not true of our example.

References

1. E. Hille, An abstract formulation of Cauchy's problem. Comptes rendus du Douzième Congrès des Mathématiciens Scandinaves, Lund, 1953, pp. 79–89.

2. L. Hörmander, Uniqueness theorems and estimates for normally hyperbolic partial differential equations of the second order. Comptes rendus du Douzième Congrès des Mathematiciens Scandinaves, Lund, 1953, pp. 105–115.

3. S. Täcklind, Sur les classes quasianalytiques des solutions des équations aux dérivées partielles du type parabolique. Nova Acta Soc. Sci. Upsal. (4) vol. 10, 1936, pp. 1–57.

4. A. Tychonov, Théorèmes d'unicité pour l'équation du chaleur, Mat. Sb., vol. 42, 1935, pp. 199–216.

ON CIRCULAR PERMUTATIONS

L. E. CLARKE, University College of Ghana and JAMES SINGER, Brooklyn College

Let a set of n objects contain r_1 elements a_1, r_2 elements a_2, $\cdots$, r_p elements a_p. The problem is to determine P, the number of circular permutations of the n objects. This problem has been discussed in the note *A general formula for circular permutations* (this MONTHLY, vol. 64, 1957, pp. 347–348), but the statement and proof of the result (Theorem 2 of the note) contain an error. For example, if $n=12$, $r_1=r_2=6$, the formula in the paper cited does not give an integral value for P; our result gives $P=80$. The error arises from improper linking of linear permutations. We obtain the circular permutations by linking d similar linear permutations, where d is any divisor of h, the greatest common divisor of $r_1, \cdots, r_p$.

THEOREM. *With the above notation*

$$P = \sum_{d \mid h} \frac{\phi(d) F_d}{n},$$

where

$$F_d = \frac{(n/d)!}{(r_1/d)! \cdots (r_p/d)!},$$

$\phi(d)$ *is Euler's function, and the summation is over all divisors* d *of* h.

Proof. Let a linear permutation of the n objects be called "*d-fold*" if it consists of d repetitions of a linear permutation of n/d of the objects; let it be called "*precisely d-fold*" if it is d-fold, but is not d_1-fold for any $d_1 > d$. It is clear that if a linear permutation is d-fold or precisely d-fold then d divides h.

The number of d-fold linear permutations is F_d; let the number of precisely d-fold linear permutations be denoted by X_d.

There is an n/d: 1 correspondence between precisely d-fold linear permuta-

tions and those circular permutations obtained by linking d (and not more than d) identical linear permutations. Therefore

$$P = \sum_{d|h} \frac{d}{n} X_d. \tag{1}$$

Further, if a d-fold linear permutation is precisely d_1-fold then d divides d_1; conversely, if d divides d_1, then a precisely d_1-fold linear permutation is also d-fold. It follows that

$$F_d = \sum_{k|h/d} X_{kd} \qquad (d \mid h). \tag{2}$$

It is necessary to solve the equations (2) for X_d $(d \mid h)$ and substitute in the equation (1). This will be done by means of the Möbius inversion formula and by use of the substitutions

$$G_d = F_{h/d}, \qquad Y_d = X_{h/d} \qquad (d \mid h). \tag{3}$$

By (2) and (3)

$$G_d = \sum_{k|d} Y_{d/k} = \sum_{k|d} Y_k. \tag{4}$$

The Möbius inversion formula applied to (4) gives

$$Y_d = \sum_{k|d} \mu\left(\frac{d}{k}\right) G_k. \tag{5}$$

By (1) and (3)

$$\begin{aligned} P &= \sum_{d|h} \frac{h}{dn} Y_d \\ &= \sum_{d|h} \frac{h}{dn} \left\{ \sum_{k|d} \mu\left(\frac{d}{k}\right) G_k \right\} && \text{(by (5))} \\ &= \sum_{k|d|h} \frac{h}{dn} \mu\left(\frac{d}{k}\right) G_k \\ &= \sum_{k|h} \frac{1}{n} G_k \left\{ \frac{h}{k} \sum_{l|h/k} \frac{\mu(l)}{l} \right\} && \text{(on putting } d = kl\text{)} \\ &= \sum_{k|h} \frac{1}{n} G_k \phi\left(\frac{h}{k}\right) = \sum_{k|h} \frac{1}{n} F_k \phi(k) && \text{(by (3)).} \end{aligned}$$

This result, though certainly not original, does not seem to be widely known. It is a particular case of a very general theorem of Pólya's (Acta Mathematica, vol. 68, 1937, pp. 145–254; Pólya's "Hauptsatz" is stated in Section 16).

A PROBLEM IN GRAPH THEORY

DONALD J. NEWMAN, AVCO Research and Advanced Development Division

Our purpose is to give a simple constructive proof of the

THEOREM. *Any graph with $2n$ vertices each of order not less than n must contain a $2n$-gon.*

A colorful interpretation of this problem is the following:

Given $2n$ people, each one a friend of at least n others (friend is reflexive), there is a way of seating them around a table such that *only* friends sit next to one another.

It is easily seen that the theorem fails if the vertices need only be of order $n-1$, for then they may form two disconnected graphs of n vertices each.

We turn now to the proof. It will be seen that despite its "*Reductio ad absurdum*" form it actually gives a construction for determining the $2n$-gon. (Seating arrangement.) This construction, furthermore, seems to be fairly economical. We shall prefer the language of the "Seating" formulation.

Proof. The trick is to introduce m new people of the Dale Carnegie type, that is, people of whom everyone is a friend. It may or may not be that with this new blood the seating is possible. It is clear, however, that if $m=2n$ it will be possible by the simple expedient of alternation. Let k, then, be the minimum m for which the seating is possible. We must prove $k=0$, so assume $k>0$, and suppose the seating arrangement to be

$$APB\cdots A$$

where P is a Dale Carnegier, and the two A's above refer to the same person. If in the sequence following the B there ever occurred an $A'B'$, (A' means friend of A, *etc.*), then forming

$$A[B\cdots A']B'\cdots A$$

and reversing those in the bracket we obtain

$$AA'\cdots BB'\cdots A,$$

an acceptable seating arrangement! [It is understood that if $B'=A$ the reversal is unnecessary.]

But, without P there can be no acceptable seating arrangement.

$\therefore$ $A'B'$ never occurs past B.

$\therefore$ $A'B'$ never occurs at all.

$\therefore$ All A' are followed by non-B',

hence number of non-B''s $\geqq$ number of A''s $\geqq n+k$. Also, number of B''s $\geqq n+k$.

Adding these two inequalities gives

$$\text{total number of people} \geqq 2n+2k,$$

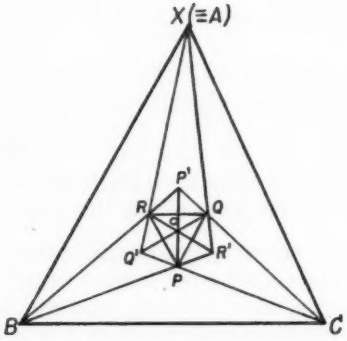
or $2n+k\geqq 2n+2k$, a contradiction since $k>0$.

AN ELEMENTARY PROOF OF MORLEY'S THEOREM

K. VENKATACHALIENGAR, Mysore University

Morley's theorem states that *the points of intersection of the adjacent trisectors of the interior angles of a triangle meet at the vertices of an equilateral triangle.*

This theorem has been proved in many ways (*cf.* [1]). We prove the result here in a simple way, using only the elementary theorems of congruence-geometry.



ABC is a triangle. First of all draw the triangle $P'BC$ with angles $P'\hat{B}C = 2/3(A\hat{B}C)$, $P'\hat{C}A = 2/3(A\hat{C}B)$ and let P be the incentre of this latter triangle (*i.e.* $P'BC$). Determine the points Q and R on CP', BP' respectively, such that $P'\hat{P}Q = P'\hat{P}R = \pi/6$. It follows that PQR is an equilateral triangle. Let O be the centre of the triangle PQR. Produce QO and RO to meet CP produced and BP produced in Q' and R' respectively, and let $Q'R$ and QR' meet in X. We shall show that X and A are identical and that the equilateral triangle PQR is the "Morley Triangle" of ABC.

From the figure we see that

$$X\hat{R}B = P'\hat{R}Q' = P'\hat{R}Q + Q\hat{R}Q'$$

$$= \frac{\pi}{2} - R\hat{P}'O + Q\hat{P}Q' = \frac{\pi}{2} - R\hat{P}'O + Q\hat{P}P' + P'\hat{P}Q'$$

$$= \frac{\pi}{2} - R\hat{P}'O + \frac{\pi}{6} + (P'\hat{C}P + P\hat{P}'C) = \frac{2\pi}{3} + \frac{C}{3},$$

and

$$X\hat{R}'B = 2R\hat{R}'P = 2\left(\pi - \frac{\pi}{6} - R\hat{P}R'\right)$$

$$= 2\left[\left(\frac{5\pi}{6}\right) - \left(\frac{\pi}{6} + P'\hat{P}R'\right)\right]$$

$$= \frac{4\pi}{3} - 2\left(\frac{B}{3} + B\hat{P}'P\right)$$

$$= \frac{4\pi}{3} - \frac{2B}{3} - \left(\pi - \frac{2B}{3} - \frac{2C}{3}\right)$$

$$= \frac{\pi}{3} + \frac{2C}{3}$$

so that

$$X\hat{R}B = \tfrac{1}{2}\pi + \tfrac{1}{2}(X\hat{R}'B). \tag{1}$$

Since RR' bisects $X\hat{R}'B$, we obtain from (1) that R is the incentre of the triangle $XR'B$. Therefore $X\hat{B}R = 1/3(A\hat{B}C)$ and $B\hat{X}R = R\hat{X}R'$ and X is on the side AB. We may see in a similar way that Q is the incentre of the triangle $XQ'C$ and therefore $X\hat{C}Q = 1/3(A\hat{C}B)$ and $C\hat{X}Q = Q\hat{X}R$ and X is on AC. Consequently, since X is on both AB and AC, $X \equiv A$. It follows that AR, AQ are the trisectors of $B\hat{A}C$ and that PQR is the "Morley Triangle" of ABC.

We see further that the triangle $P'RQ$, $Q'PR$, $R'QP$ are all isosceles with their equal angles given by $1/3(B+C)$, $1/3(C+A)$, $1/3(A+B)$ respectively, if A, B, C denote the angles of the original triangle ABC. Therefore $A\hat{R}Q = 1/3(\pi+B)$ and we may now determine the side of the Morley triangle on employing the relations

$$a \operatorname{cosec} A = b \operatorname{cosec} B = c \operatorname{cosec} C = 2\rho = \text{circular diameter}$$

for a triangle. We check the well-known formula

$$PQ = QR = RP = 8\rho \sin\frac{A}{3} \sin\frac{B}{3} \sin\frac{C}{3}.$$

Reference

1. Clarence Lubin, A proof of Morley's theorem, this MONTHLY, vol. 62, 1955, pp. 110–112. (Also the references contained therein.)

A WARNING ABOUT TRANSLATING AXIOMS*

H. Hiż, Pennsylvania State University

In a recent paper [1] Halmos used conjunction (A) and negation (N) as primitives of the sentential calculus and considered disjunction and implication between s and t as abbreviations for $NANsNt$ and $NAsNt$ respectively. As

* This paper was written while the author was engaged in a research project sponsored by the National Science Foundation.

axioms for the (A, N) system, he took the standard [2] set based on disjunction and negation as primitives and considered them as abbreviations for

(1) $NANANsNsNs$,
(2) $NAsNNANsNt$,
(3) $NANANsNtNNANtNs$,
(4) $NANAsNtNNANANuNsNNANuNt$.

The rule of inference (without abbreviations) states that if s and $NAsNt$ are tautologies, then t is a tautology.

However, this set of axioms is not complete. To see this consider the following three-valued interpretation of A and N where 1 is the only designated value:

A	1	2	3	N
*1	1	1	3	3
2	2	2	3	1
3	3	3	3	1

The rule of inference leads from expressions assigned the designated value to expressions assigned the designated value. The axioms (1)–(4) take the designated value always. But $NANss$ (which is a tautology) assumes the value 3 when one uses 2 for s. Thus, $NANss$ does not follow from the axioms. Similarly, *e.g.*, $NANsAst$, $NAAstNNNAsNNt$ are not provable. Note that in checking the fact that (1)–(4) assume always 1 and that the rule leads from $s=NAsNt=1$ to $t=1$, one never uses the equality $A12=1$ (this results from the circumstance that a nonnegated variable never occurs in the axioms as the second argument of A), which is essentially involved in the quoted examples of unprovable tautologies. Still, addition of, *e.g.*, $NANAstNNAtNNs$ would leave the quoted tautologies unprovable. For complete axiomatisations of (A, N) consult [3] and [4]. Note also that $NAAstNNNAsNNt$ can be considered as a part of the definition of conjunction by implication (C) and negation: $Ast=NCsNt$ (write it as an implication and translate into (A, N) language). A translation of a complete set of axioms to another set of primitives would be complete only if from the resulting axioms the definitions of the first set of primitives followed.

This mistake is of no consequence for the totality of Halmos' paper where the considerations about the axiomatic setup of the sentential calculus were only parenthetical. Halmos himself raised (in a conversation) the problem of completeness of the translated axiomatisation; the possibility that the answer might be negative was first signaled by J. B. Rosser (in a letter to Halmos).

References

1. Paul R. Halmos, The basic concepts of algebraic logic, this MONTHLY, vol. 63, 1956, p. 368.
2. D. Hilbert and W. Ackermann, Principles of Mathematical Logic, New York, 1950, p. 27.
3. Bolesław Sobociński, Axiomatisation of a conjunctive-negative calculus of propositions. J. Computing Systems, vol. 1, 1954, pp. 229–242. (This is a translation of a paper from Collectanea Logica, vol. 1, 1939.)
4. J. Barkley Rosser, Logic for Mathematicians, New York, 1953, p. 55.

CLASSROOM NOTES

EDITED BY C. O. OAKLEY, Haverford College

All material for this department should be sent to C. O. Oakley, Department of Mathematics, Haverford College, Haverford, Pa.

ON SOME THEOREMS ON PERMUTATIONS

W. A. AL-SALAM, Duke University

Recently Mullin [1] discussed the function

$$\Phi(n) = \sum_{r=0}^{n} {}_nP_r$$

where n is a nonnegative integer and ${}_nP_r = n!/(n-r)!$.

It might be of interest to consider the more general function

$$\Phi_k(n) = \sum_{k=0}^{n} \{{}_nP_r\}^k, \quad k \text{ a positive integer.}$$

We have the following theorems:

THEOREM 1. *A canonic generator for Φ_k is*

$$\Phi_k(n+1) = (n+1)^k \Phi_k(n) + 1.$$

Proof. We have

$$\Phi_k(n+1) = \sum_{r=0}^{n+1} \frac{((n+1)!)^k}{(r!)^k} = (n+1)^k \sum_{r=0}^{n+1} \left(\frac{n!}{r!}\right)^k = (n+1)^k \Phi_k(n) + 1.$$

THEOREM 2. *An asymptotic expansion for $\Phi_k(n)$ is*

$$\Phi_k(n) \sim (n!)^k \, {}_oF_{k-1}(1, 1, \cdots, 1; 1)$$

where, in the notation of the hypergeometric functions,

$${}_oF_{k-1}(\alpha_1, \cdots, \alpha_{k-1}; z) = \sum_{r=0}^{\infty} \frac{z^r}{r!(\alpha_1)_r \cdots (\alpha_{k-1})_r},$$

$$(\alpha)_r = \alpha(\alpha+1) \cdots (\alpha+r-1) \qquad (r \geq 1),$$

$$(\alpha)_o = 1.$$

${}_oF_k(\alpha_1, \cdots, \alpha_k; z)$ converges for all z.

Proof.

$$\Phi_k(n) = (n!)^k \left\{ \sum_{r=0}^{\infty} \left(\frac{1}{r!}\right)^k - \sum_{r=n+1}^{\infty} \left(\frac{1}{r!}\right)^k \right\}$$

$$= (n!)^k \, {}_oF_{k-1}(1, 1, \cdots, 1; 1) + o((n!)^k).$$

THEOREM 3.

$$\Phi_k(n) \sim (2\pi)^{k/2} n^{k(n+1/2)} e^{-kn} {}_0F_{k-1}(1, 1, \cdots, 1; 1).$$

Proof. As in [1] this theorem follows from Sterling's formula and Theorem 2.

Now let $J_0(x)$ be the Bessel function of order zero. It is given by

$$J_0(x) = {}_0F_1\left(1; -\frac{x^2}{4}\right).$$

In particular we find from the tables that $J_0(2i) = 2.280$.

We have the following corollary to Theorems 2 and 3:

COROLLARY.

$$\Phi_2(n) = \sum_{r=0}^{n} \{{}_nP_r\}^2 \sim 2.280(n!)^2$$

$$\sim 4.560\pi \cdot n^{2n+1} \cdot e^{-2n}.$$

In this connection we also note that

$$\sum_{r=0}^{n} {}_nP_r \, {}_nC_r = L_n(-1),$$

where $L_n(x)$ is the Laguerre polynomial of order zero [2].

References

1. A. A. Mullin, Three theorems on permutations, this MONTHLY, vol. 64, 1957, pp. 669–670.
2. D. V. Widder, Advanced Calculus, New York, 1947, p. 383.

AN ANALYTIC APPROACH TO TRIGONOMETRIC FUNCTIONS

D. A. KEARNS, Merrimack College

Consideration of the elementary functions from purely analytic points of view can provide excellent instructional material. Unfortunately, although such developments occur here and there in mathematical literature, they may be inaccessible to many students and to some teachers, either because they are written in languages other than English or are found in texts of a fairly advanced nature.

In this note we deal with the sine and cosine functions, deriving their major properties from the equation for simple harmonic motion and without the introduction of infinite series. The few properties of linear differential equations needed can be made at least plausible even to students having only an elementary background in calculus.

We begin by considering the differential equation

$$\frac{d^2y}{dx^2} + y = 0. \tag{1}$$

By a solution of this equation we shall mean a continuous function, $y(x)$, which satisfies (1) and which has a continuous first derivative. The fundamental existence and uniqueness theorems of the theory of ordinary differential equations apply to (1). In particular, *there exists one and only one solution, $y(x)$, of* (1) *such that $y(x_0)=y_0$ and $y'(x_0)=y_0'$, where x_0, y_0, y_0' are arbitrary constants.* Geometrically, this says that there is one and only one curve passing through (x_0, y_0) with a slope of y_0' at this point, the equation of which satisfies (1).

Two solutions of (1), $y_1(x)$ and $y_2(x)$, are called linearly independent if the identity $c_1y_1(x)+c_2y_2(x)\equiv 0$ implies $c_1=c_2=0$.

The only other result we use from the theory of differential equations is the fact that any solution of (1) can be expressed as a linear combination of two linearly independent solutions. That is, if $y(x)$ is a solution of (1) and $y_1(x)$ and $y_2(x)$ are linearly independent solutions, then there are constants c_1 and c_2 such that $y(x)=c_1y_1(x)+c_2y_2(x)$.

Let us then consider two solutions of (1), $y=s(x)$ and $y=c(x)$ such that

$$s(0) = 0, \qquad s'(0) = 1; \tag{2}$$

and

$$c(0) = 1, \qquad c'(0) = 0. \tag{3}$$

THEOREM 1. *$s(x)$ and $c(x)$ are linearly independent.*

Proof. Suppose there are constants, c_1 and c_2, such that $c_1s(x)+c_2c(x)\equiv 0$. Then $c_1s'(x)+c_2c'(x)\equiv 0$.

In particular these identities hold when $x=0$, so that $c_1s(0)+c_2c(0)=0$ and $c_1s'(0)+c_2c'(0)=0$.

These equations together with (2) and (3) imply $c_1=c_2=0$.

THEOREM 2. $s'(x)=c(x)$.

Proof. Since $s(x)$ is a solution of (1), we must have $s''(x)+s(x)=0$. Just as this equation defines $s''(x)$ as a continuous function, the equation $s'''(x)+s'(x)=0$ shows that $s'''(x)$ exists and is continuous. Letting $y=s'(x)$, the last equation becomes equation (1). Furthermore, $y(0)=s'(0)=1$ by (2). Since $y'(x)=s''(x)=-s(x)$, it follows that $y'(0)=0$. Thus $y=s'(x)$ is a solution of (1) satisfying equations (3). But there is only one such function because of the uniqueness asserted by the theorem quoted above. Since $c(x)$ is this function, $s'(x)\equiv c(x)$.

THEOREM 3. $c'(x)=-s(x)$.

Proof. $c'(x)=s''(x)=-s(x)$ by Theorem 2 and equation (1).

THEOREM 4. $s^2(x)+c^2(x)\equiv 1$.

Proof. Since $s(x)$ satisfies (1), $s''(x)+s(x)=0$.

Multiplying this by $s'(x)$ we obtain, $s'(x)s''(x)+s'(x)s(x)=0$. Integrating,

it follows that $(s'(x))^2+(s(x))^2=$constant, or $c^2(x)+s^2(x)=$constant. But at $x=0$, because of (2) and (3), $c^2(0)+s^2(0)=1$. Therefore, $s^2(x)+c^2(x)\equiv 1$.

THEOREM 5. *For arbitrary* a, $s(x+a)=s(x)c(a)+s(a)c(x)$.

Proof. Since $s(x)$ is a solution of (1), so is $s(x+a)$. Therefore $s(x+a)$ can be expressed as a linear combination of the linearly independent solutions $s(x)$ and $c(x)$. That is, there are constants, c_1 and c_2, such that

$$s(x+a)=c_1s(x)+c_2c(x). \tag{4}$$

At $x=0$, this becomes $s(a)=c_1s(0)+c_2c(0)=c_2$, where we have used (2) and (3). Differentiating (4), we obtain

$$c(x+a)=c_1c(x)-c_2s(x). \tag{5}$$

Again letting $x=0$ and using (2) and (3), $c(a)=c_1c(0)-c_2s(0)=c_1$. Substituting these values for c_1 and c_2 in (4) yields the desired identity.

THEOREM 6. *For arbitrary* a, $c(x+a)=c(x)c(a)-s(x)s(a)$.

Proof. Substitute the c_1 and c_2 obtained in the proof of Theorem 5 in (5).

THEOREM 7. $s(-x)=-s(x)$ *and* $c(-x)=c(x)$.

Proof. Letting $a=-x$ in the identities of Theorems 5 and 6, we obtain two linear equations in $s(-x)$ and $c(-x)$:

$$s(x)c(-x)+c(x)s(-x)=0,\ c(x)c(-x)-s(x)s(-x)=1.$$

Since the determinant of this system is $-s^2(x)-c^2(x)=-1\neq 0$, we may solve the equations for $s(-x)$ and $c(-x)$ to obtain the theorem.

THEOREM 8. $s(x)$ *has at least one relative maximum point.*

Proof. Since $s(0)=0$, $s'(0)=1$, and $s(x)$ and $s'(x)$ are continuous functions, there is a neighborhood to the right of $x=0$ in which $s(x)$ is positive and monotonically increasing. As x becomes positively infinite, $s(x)$ must behave in one of the following mutually-exclusive ways:

(i) $s(x)$ becomes positively infinite monotonically;
(ii) $s(x)$ approaches a horizontal asymptote monotonically;
(iii) $s(x)$ has a relative maximum point for some positive value of x.

We show that (i) and (ii) are impossible.

Elimination of the first case follows immediately from Theorem 4. Since $s^2(x)+c^2(x)\equiv 1$, $s(x)$ is bounded.

To eliminate the possibility of (ii), suppose it to be true. It would then follow that

$$\lim_{x\to\infty} s'(x)=\lim_{x\to\infty} c(x)=0,$$

which implies

$$\lim_{x\to\infty} c(x+a) = 0 \text{ for arbitrary } a,$$

and

$$\lim_{x\to\infty} s(x) = \lim_{x\to\infty} \sqrt{1-c^2(x)} = 1.$$

But then,

$$\lim_{x\to\infty} c(x+a) = \lim_{x\to\infty} (c(x)c(a) - s(x)s(a)) = -s(a).$$

Since $s(x)$ is not identically zero, this is a contradiction.

Therefore, (iii) must be the case.

Remark. Since $c(x)$ is continuous and not identically zero, there must be a smallest positive value of x for which $s'(x)=c(x)=0$. We shall designate this value by $\frac{1}{2}p$ and note that $c(\frac{1}{2}p)=0$ and $s(\frac{1}{2}p)=1$.

THEOREM 9. *$s(x)$ and $c(x)$ are periodic with period $2p$. That is, for any x, $s(x+2p)=s(x)$ and $c(x+2p)=c(x)$.*

Proof. $s(x+\frac{1}{2}p) = s(x)c(\frac{1}{2}p) + s(\frac{1}{2}p)c(x) = c(x)$, and $c(x+\frac{1}{2}p) = c(x)c(\frac{1}{2}p) - s(x)s(\frac{1}{2}p) = -s(x)$. Therefore,

$$s(x+p) = c(x+\tfrac{1}{2}p) = -s(x), \tag{6}$$

and $c(x+p)=-s(x+\frac{1}{2}p)=-c(x)$. It follows that $s(x+2p)=-s(x+p)=s(x)$ and $c(x+2p)=-c(x+p)=c(x)$.

THEOREM 10. *$2p$ is the smallest period of $s(x)$ and $c(x)$.*

Proof. By (6) and Theorem 7,

$$s(\tfrac{1}{2}p - x) = -s(x-\tfrac{1}{2}p) = s(x+\tfrac{1}{2}p),$$

so that $s(x)$ is symmetric with respect to the line $x=\frac{1}{2}p$. Now suppose there exists a P smaller than $2p$ but greater than zero such that $s(x+P)\equiv s(x)$. Then $s(P)=s(0)=0$. Because of the symmetry proven above, p is the smallest positive zero of $s(x)$. Therefore $P=p$. But p is not a period of $s(x)$, and hence neither is P.

THEOREM 11. $p=\pi$.

Proof. The curve $u=c(x)$, $v=s(x)$, $0\leqq x\leqq 2p$, represents a unit circle in the u, v-plane the circumference of which is given by

$$s = \int_0^{2p} \sqrt{(s'(x))^2 + (c'(x))^2}\,dx = \int_0^{2p} dx = 2p.$$

Hence, $2p=2\pi$.

Remarks. This last proof points directly to a geometric interpretation of the functions $u=c(x)$ and $v=s(x)$. The curve $u^2+v^2=1$ is a unit circle. Any point on this circle has an abscissa, $c(x)$, and an ordinate, $s(x)$. The angle which the radius vector to any point (u, v) makes with the positive u-axis is x since the subtended arc is given by

$$\int_0^x (s^2(t) + c^2(t))^{1/2}\, dt = \int_0^x dt = x.$$

The infinite series expansions of $s(x)$ and $c(x)$ can be found in the usual way. That is, we try to find functions $y=\sum a_n x^n$ which satisfy (1), and (2) or (3). The resulting series and their derivatives converge, and by the uniqueness of solutions of these differential systems, are identical to $s(x)$ and $c(x)$ respectively.

Reference

W. F. Osgood, Lehrbuch der Funktionentheorie, I, Leipzig and Berlin, 1912.

THE INDEPENDENCE OF THE ASSOCIATIVE LAW

L. O. Kattsoff, Harpur College

Independence proofs are not indispensable, to judge by their absence in various algebras. Quite often textbooks on abstract algebras or discussions of geometric postulates pay lip-service to the concept and then add that they will not show the independence of all the postulates. Historically, of course, independence proofs, or attempts at them, have been quite fruitful in revealing varieties of algebras and diversities of geometric systems.

The existence of nonassociative algebras is quite intriguing. An easy way to show that existence is to exhibit the independence of the associative law from the remaining postulates for the group. This is not too difficult if we also give up the commutative law. However, to show independence in the case of an Abelian group seems to be more difficult. I offer the following as demonstration of the independence of the associative law in an Abelian group.

Postulates: Given the set G containing elements $a, b, c, \cdots$, and a binary operation $\circ$ on G:

1. For every pair of elements a and b, $a \circ b$ is in G.
2. For any three elements a, b, and c, $(a \circ b) \circ c = a \circ (b \circ c)$.
3. There exists an element i in G such that $a \circ i = i \circ a = a$.
4. For every element a there exists an element a^{-1} in G, such that $a \circ a^{-1} = a^{-1} \circ a = i$.
5. For any two elements a and $b(a, b \neq i)$, $a \circ b = b \circ a$; if $a=b=i$, $i \circ i = i$.

To show the independence of Postulate 2, the associative law, and hence to show the consistency of the remaining set with the denial of Postulate 2, we construct nonassociative algebras in this fashion.

A) Consider the infinite set G:

$$\{i, 1, 2, 3, 4, \cdots 1^{-1}, 2^{-1}, 3^{-1}, 4^{-1} \cdots\}.$$

Let max (a, b) designate that element a or b, that lies furthest to the right in G.

$a \circ b$ designates the successor of max (a, b)

when $a, b \neq i$ and $b \neq a^{-1}$.

We further define:

(I) $a \circ b = a$ when $b = i$,
(II) $a \circ b = i$ when $b = a^{-1}$,
(III) $a \circ b = i$ when $a = b = i$.

It is evident that $a \circ b$ is commutative from its definition, and Postulate 5 is satisfied.

I and II define i as the identity element, and hence Postulate 3 is satisfied.

Postulate 2 is not satisfied since if $a = 2$, $b = 3$, $c = 4$,

$$(a \circ b) \circ c \neq a \circ (b \circ c),$$
$$(2 \circ 3) \circ 4 \neq 2 \circ (3 \circ 4),$$
$$4 \circ 4 \neq 2 \circ 5,$$
$$5 \neq 6.$$

B) Consider $G = \{0, 1, 2, \cdots\}$.

We define max (a, b) as above, and note that this may simply mean the ordinary definition of "greater than" in the natural number series.

$a \circ b$ designates the successor of max (a, b)

when $a \neq b$, $a > 0$, $b > 0$.

We further define

(I) $a \circ b = 0$, when $a = b$,
(II) $a \circ b = a$, when $b = 0$,
(III) $a \circ b = b$, when $a = 0$.

All the postulates are satisfied except the associative law since

$$2 \circ (3 \circ 4) = 2 \circ 5 = 6$$

while

$$(2 \circ 3) \circ 4 = 4 \circ 4 = 0.$$

C) Consider $G = \{0, 1, 2, \cdots, n\}$ and an operator $t(a)$ defined in this way:

$$t(a) \text{ designates } \begin{cases} a + 1 \text{ when } a \neq n, \\ 1 \text{ when } a = n. \end{cases}$$

$a \circ b$ is defined as above in **B**).

This set is nonassociative for $n>2$.

Set C is intrinsically interesting because it is a finite set.

Both B) and C) differ from A) in that, in each of these, each element is its own inverse, while in the first example each element (except i) has a distinct inverse.

The following postulates for a nonassociative algebra suggest themselves:

(i) 1 is a number.

(ii) To every pair of numbers a and b in G, there is a number $a \circ b$ in G.

(iii) There are no numbers a and b such that $a \circ b = 1$.

(iv) If the numbers a, b, c, d are such that $a \circ b = c \circ d$, then $\max(a, b) = \max(c, d)$.

(v) If a set of numbers contains 1 and if whenever it contains a and b it contains $a \circ b$, then it contains all numbers.

ON THE DEFINITION OF ln a

S. LEADER, Rutgers University

In defining the natural logarithm by the definite integral

$$\ln a = \int_1^a x^{-1}dx \tag{1}$$

for $a>0$, the logarithmic properties of $\ln a$ can be derived quite simply by first proving

$$\ln a = \lim_{h\to 0} \frac{a^h - 1}{h}. \tag{2}$$

To prove (2) note that for $b>1$ and $1/b \leqq x \leqq b$ we have $\left|x^{h-1} - x^{-1}\right| = x^{-1}\left|x^h - 1\right| \leqq b(b^{|h|} - 1)$ for all h. Hence, $\lim_{h\to 0} x^{h-1} = x^{-1}$ uniformly in $[1/b, b]$. This implies

$$\int_1^a x^{-1}dx = \lim_{h\to 0} \int_1^a x^{h-1}dx. \tag{3}$$

Now for $h \neq 0$,

$$\int_1^a x^{h-1}dx = \frac{x^h}{h}\Big]_1^a = \frac{a^h - 1}{h}. \tag{4}$$

So (2) follows from (1), (3), and (4). The logarithmic properties of $\ln a$ can be derived from (2) in the following way.

$$\ln ab = \lim_{h\to 0} \frac{(ab)^h - 1}{h} = \lim_{h\to 0} \frac{a^h b^h - b^h + b^h - 1}{h}$$

$$= \lim_{h\to 0}\left(\frac{a^h-1}{h}\right)b^h + \left(\frac{b^h-1}{h}\right)$$

$$= \left(\lim_{h\to 0}\frac{a^h-1}{h}\right)\left(\lim_{h\to 0} b^h\right) + \left(\lim_{h\to 0}\frac{b^h-1}{h}\right)$$

$$= \ln a + \ln b.$$

$$\ln a^c = \lim_{h\to 0}\frac{a^{ch}-1}{h} = \lim_{h\to 0} c\left(\frac{a^{ch}-1}{ch}\right) = c\lim_{p\to 0}\frac{a^p-1}{p}$$

$$= c \ln a, \text{ where } p = ch \text{ and } c \neq 0.$$

Thus, defining e by $\ln e = 1$, we have $\ln e^x = x \ln e = x$. So $\ln a$ is the logarithm of a to the base e.

To obtain the differentiation formula for a^x multiply (2) by a^x:

$$a^x \ln a = a^x \lim_{h\to 0}\frac{a^h-1}{h} = \lim_{h\to 0}\frac{a^x(a^h-1)}{h} = \lim_{h\to 0}\frac{a^{x+h}-a^x}{h} = \frac{d}{dx}a^x.$$

[For related ideas see *A note on the base of natural logarithms* by E. Leach, this MONTHLY, vol. 60, 1953, p. 622.]

NOTE ON A PAPER BY R. STEINBERG

HERBERT J. CURTIS, University of Illinois

In his Classroom Note *Note on linear differential equations* (January, 1957) R. Steinberg suggests a method for finding particular solutions of certain linear differential equations.

It should be noted that this method fails to yield a particular solution of such a simple equation as $(D-1)z = e^x$, nor indeed of any equation $f(D)z = u$, if the polynomial f is a divisor of g. In this case $k = 1$, $h = f$, and the method requires that we know a particular solution of $h(D)v = u$. But this equation is equivalent to $f(D)z = u$.

Moreover, *only* if f and g are relatively prime will the method yield solutions. Unless f and g are relatively prime, h and g have a common factor of degree greater than zero. To find a solution of $h(D)v = u$ we apply the method again and split h into two factors, h_1 and k_1, with k_1 relatively prime to g. Then h_1 and g have a common factor of degree greater than zero. Ultimately we are faced with the necessity of obtaining a particular solution of an equation $h_n(D)v = u$ with h_n a factor of g. But such a solution the method will not give.

The important part of Steinberg's theorem is the statement that there exists a solution of $f(D)z = u$ which is also a solution of $g(D)h(D)z = 0$. This is essentially the basis of the method of undetermined coefficients given, for example, in Rainville's *Elementary Differential Equations*, page 108 and following.

PARTICULAR INTEGRALS FOR NONHOMOGENEOUS, LINEAR, ORDINARY DIFFERENTIAL EQUATIONS

G. E. LATTA, Stanford University

In standard references which treat elementary integration techniques for ordinary linear differential equations, the methods given for obtaining particular integrals include variation of parameters, and special procedures for constant coefficient equations. The role of the adjoint equation in this context seems to be almost completely overlooked and, indeed, the adjoint equation is seldom used in elementary courses on this subject. However, a straightforward application of the adjoint equation leads to a well-motivated construction of a particular integral, and the method has certain advantages.

In the following, let

$$Ly \equiv y^{(n)} + p_1(x)y^{(n-1)} + \cdots + p_n(x)y = r(x) \tag{1}$$

be a given linear equation. The adjoint expression corresponding to Ly is

$$\bar{L}v = (-1)^n v^{(n)} + (-1)^{n-1}(p_1(x)v)^{(n-1)} + \cdots - (p_{n-1}(x)v)' + p_n(x)v \tag{2}$$

and we may introduce the adjoint equation by trying to construct an integrating factor for the expression Ly; *i.e.*, $v(x)Ly$ is to be a total derivative. Thus

$$vLy = \frac{d}{dx}\{P(y, v)\} + y\bar{L}v \tag{3}$$

is Lagrange's identity, $\bar{L}v$ the adjoint of Ly, and $P(y, v)$ is a bilinear expression, linear in $y, y', \cdots, y^{(n-1)}$, and $v, v', \cdots, v^{(n-1)}$, called the bilinear concomitant. In this way, v is an integrating factor for Ly provided $\bar{L}v = 0$. Since the adjoint of $\bar{L}v$ is Ly, we see that, reciprocally, y is an integrating factor of $\bar{L}v$ if $Ly = 0$.

An immediate consequence of (3) is that if we know all the solutions of $Ly = 0$, then the solutions of $\bar{L}v = 0$ can be obtained by purely algebraic means. To see this, let $y_1, \cdots, y_n$ be a set of linearly independent solutions of $Ly = 0$. Then (3) becomes

$$vLy_i = \frac{d}{dx}\{P(y_i, v)\} + y_i\bar{L}v = 0 \qquad i = 1, \cdots, n,$$

since $Ly_i = 0$. To solve $\bar{L}v = 0$, we have

$$\frac{d}{dx}\{P(y_i, v)\} = 0, \quad \text{or} \quad P\{y_i, v\} = c_i \qquad i = 1, \cdots, n. \tag{4}$$

Equations (4) are a set of n linear algebraic equations in $v, v', \cdots, v^{(n-1)}$. An elementary calculation shows that the determinant of the coefficients of $v, v', \cdots, v^{(n-1)}$ in these equations is

$$\pm \begin{vmatrix} y_1 & y_1' \cdots y_1^{(n-1)} \\ \cdot & \\ \cdot & \\ y_n & y_n' \cdots y_n^{(n-1)} \end{vmatrix} = \pm W(y_1, \cdots, y_n),$$

the Wronskian of $y_1, \cdots, y_n$, and is thus nonzero. Using Cramer's rule, we find $v(x)$ as a quotient of determinants, involving n arbitrary constants $c_1, \cdots, c_n$, and is thus the general solution of $\bar{L}v=0$.

To find a particular integral of $Ly=r(x)$, we assume that we know the solutions $y_1, \cdots, y_n$ of the homogeneous equation, or, equivalently, $v_1, \cdots, v_n$ of $\bar{L}v=0$. Then (3) becomes

$$v_i Ly = \frac{d}{dx}\{P(y, v_i)\} + y\bar{L}v_i \qquad i = 1, \cdots, n, \qquad \frac{d}{dx}\{P(y, v_i)\} = v_i r(x)$$

and integrating,

$$P(y, v_i) = \int^x v_i(t)r(t)dt + c_i. \tag{5}$$

Proceeding as above, we can solve for y as the quotient of two determinants, and may take each $c_i=0$ if we merely desire a particular integral. If we wish to solve the initial value problem, given $y, y', \cdots y^{(n-1)}$ at x_0, then (5) becomes

$$P(y, v_i) = \int_{x_0}^x v_i(t)r(t)dt + c_i$$

and the c_i are given immediately in terms of the initial values. For example $Ly=y''+y=\sec x$ and Ly is self adjoint,

$$\sin x(y'' + y) = \frac{d}{dx}(y' \sin x - y \cos x) = \frac{\sin x}{\cos x},$$

$$\cos x(y'' + y) = \frac{d}{dx}(y' \cos x + y \sin x) = 1,$$

$$y' \sin x - y \cos x = -\log \cos x,$$

$$y' \cos x + y \sin x = x.$$

Thus $y=x \sin x+\cos x \log \cos x$ is a particular integral.

SELF-INTERSECTIONS OF SPECIAL CURVES

W. Funkenbusch, Michigan College of Mining and Technology

The curves we consider are defined by $x=f(t)$, where $f(h+k)=f(h-k)$, h being a constant, and y being an nth degree polynomial in t designated by $\phi(t)$. The plotting of these curves from their parametric equations may be expedited by the following direct method for finding points of self-intersection.

Let us define $\psi(t)=\phi(t+h)$. In order that the two t values, $t=h\pm k$, produce the same y in addition to producing the same x, it is required that $\psi(k)=\psi(-k)$. This means that the desired values of k are the nonzero zeros of $\theta(k)$, where $\theta(k)$ contains the odd degree terms of $\psi(k)$. Obviously $\theta(0)=0$, and therefore if $n<11$, we need to solve no higher than a fourth degree equation in k^2.

Example. Find any self-intersection points on the curve $x=t^2-4t$, $y=\phi(t)=t^3-2t^2-7t$.

Solution. We have $h=2$, $t=2\pm k$, $\psi(t)=t^3+4t^2-3t-14$, $\theta(k)=k^3-3k$, and $k=0$ or $\pm\sqrt{3}$. Hence $t=2\pm\sqrt{3}$, gives the point $(-1, -2)$ as a point of self-intersection.

Other problems with solutions are as follows:

(1)
$$x=\frac{1}{1+t^2}, \qquad y=t^3-t-6,$$
$$t=\pm 1, \text{ gives } \left(\frac{1}{2}, -6\right).$$

(2)
$$x=\frac{e^t+e^{-t}}{2}, \qquad y=t^3-t-6,$$
$$t=\pm 1, \text{ gives } \left(\frac{e^2+1}{2e}, \frac{e^2+1}{2e}\right).$$

(3)
$$x=t^2-2t, \qquad y=t^5-3t^4-5t^3+15t^2+4t-12$$
$$t=-1 \text{ or } 3 \text{ gives } (3, 0) \text{ and } t=1\pm\sqrt{3} \text{ gives } (2, -6).$$

(4)
$$x=\cos t, \qquad y=t^3-3t^2-3t$$
$$t=\pm\sqrt{3} \text{ gives } (\cos\sqrt{3}, -9).$$

MATHEMATICAL EDUCATION NOTES

Mathematical Education Notes, a new department of the MONTHLY will appear for the first time in the November, 1958, issue. Editors of the department are John R. Mayor, American Association for the Advancement of Science and the University of Maryland, and John A. Brown, University of Delaware. Contributions should be addressed to Mr. Mayor, 1515 Massachusetts Avenue, N.W., Washington 5, D. C.

The national interest in the improvement of science education, perhaps greatest in mathematics as one of the sciences, is increasing. Already much work has been done to improve mathematics education, particularly in grades 9 to 12 and in the first two years of college. But a very great deal remains to be

done. A considerable share of the work, on which improvement can be based, must be carried by members of the Mathematical Association of America. It is hoped that this department may strengthen this effort in providing information and points of view on curriculum in mathematics and the other sciences, experimental studies in progress, educational uses of films and television, educational activities of professional societies, and other reports of importance to mathematics education.

ELEMENTARY PROBLEMS AND SOLUTIONS

EDITED BY HOWARD EVES, University of Maine

Send all communications concerning Elementary Problems and Solutions to Howard Eves, Mathematics Department, University of Maine, Orono, Maine. This department welcomes problems believed to be new, and demanding no tools beyond those ordinarily furnished in the first two years of college mathematics. To facilitate their consideration, solutions should be submitted on separate, signed sheets, within three months after publication of problems.

PROBLEMS FOR SOLUTION

E 1331. *Proposed by P. L. Duren, Massachusetts Institute of Technology*

Show that, for all $a \geqq 0$ and $b \geqq 1$,

$$ab \leqq e^a + b(\ln b - 1),$$

with equality if and only if $b = e^a$.

E 1332. *Proposed by P. L. Chessin, University of Maryland*

If A, B, C are the angles of a triangle and x is such that

$$\cos(x + A)\cos(x + B)\cos(x + C) + \cos^3 x = 0,$$

then

(1) $$\tan x = \cot A + \cot B + \cot C,$$

(2) $$\sec^2 x = \csc^2 A + \csc^2 B + \csc^2 C.$$

E 1333. *Proposed by V. F. Ivanoff, San Carlos, California*

If $s_k = 1^k + 2^k + \cdots + n^k$, show that

$$\begin{vmatrix} s_1 & 1 & 0 & 0 & \cdot & 0 \\ s_2 & s_1 & 2 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ s_{n-1} & s_{n-2} & \cdot & \cdot & \cdot & n \\ s_n & s_{n-1} & \cdot & \cdot & \cdot & s_1 \end{vmatrix} = (n!)^2.$$

E 1334. *Proposed by Burton Randol, The Rice Institute*

If $f(z)$ is any simply periodic entire function, show that there exists a (finite) z_0 such that $f(z_0)=z_0$.

E 1335. *Proposed by C. N. Campopiano, Polytechnic Institute of Brooklyn*

Let $f(z)$ be a complex function of the complex variable z defined for all finite z. Suppose there is a constant k, $0<k<1$, such that

$$|f(z)-f(w)| \leqq k|z-w|$$

for all z, w. Show that there is a unique solution to the equation

$$z=f(z)+a,$$

where a is an arbitrary constant.

SOLUTIONS

A Triangle with Angles in Geometric Progression

E 1301 [1958, 122]. *Proposed by Victor Thébault, Tennie, Sarthe, France*

If the angles of a triangle ABC are consecutive terms of a geometric progression of common ratio 3, then

$$\cos B \cos C+\cos C \cos A+\cos A \cos B=-1/4.$$

Solution by M. T. Salhab, Carnegie Institute of Technology. We may take $A=3B=9C$, $C=\pi/13$. Using $\cos x \cos y=[\cos(x+y)+\cos(x-y)]/2$, we have to show that

$$\sum_{k=1}^{6} \cos 2kC=-1/2.$$

Now using

$$\sum_{k=1}^{n} \cos 2k\theta=\frac{\sin(2n+1)\theta}{2\sin\theta}-\frac{1}{2}$$

with $n=6$, $\theta=\pi/13$, the desired result follows immediately.

Also solved by A. N. Aheart, R. G. Albert, J. B. Baird III, Edward Barbeau, B. H. Bissinger, L. R. Bragg, Julian Braun, D. R. Brillinger, Thédose Brown, C. S. Carlson, P. L. Chessin, A. G. Clark, J. W. Clawson, Mary Dean Clement, A. E. Danese, J. E. Darraugh, E. L. Ellis and D. L. Muench (jointly), G. W. Erwin, Jr., P. A. Fillmore and E. H. Kanning III (jointly), Leona Freeman, Jose Gallego-Diaz, H. S. Gaples, Jr., L. L. Garner, Michael Goldberg, S. H. Greene, J. W. Haake, A. R. Hyde, M. S. Klamkin, J. D. E. Konhauser, Morton Kupperman, Leon Lefton, Joe Lipman, R. L. London, D. C. B. Marsh, C. T. Molloy, Jr., J. B. Muskat, E. F. Myers, F. D. Parker, L. A. Ringenberg, Jeff Ritterman, D. A. Robinson, Azriel Rosenfeld, Nathan Schwid, T. H. Slook, R. H. Sprague, W. B. Stovall, Jr., Harry Weingarten, Ralph Wiggins, Samuel Wolf, Dale Woods, Roscoe Woods, J. W. Young, David Zeitlin, the proposer, and two anonymous solvers.

Garner proposed the allied problem: If the angles A, B, C, D of a (reëntrant) quadrilateral $ABCD$ are consecutive terms of a geometric progression of common ratio 3, then

$$\cos A \cos B + \cos B \cos C + \cos C \cos D + \cos D \cos A = 1/2.$$

Locus of a Centroid

E 1302 [1958, 122]. *Proposed by M. S. Klamkin, AVCO, Research and Development, Lawrence, Mass.*

A square is divided into two parts by an arbitrary diameter through its center. Determine the locus of the centroid of one of the equal areas.

Solution by B. H. Bissinger, Lebanon Valley College. Consider the square with vertices at $(\pm 1, \pm 1)$. Taking moments about the coordinate axes we find the centroid of the region below the diameter of slope m, $|m| \leqq 1$, has coordinates $x = m/3$, $y = -1/2 + m^2/6$. Considerations of symmetry prove the closed path of the centroid for one complete revolution of the diameter consists of four parabolic sections whose equations are

$$4y^2 = (3x^2 - 1)^2, \qquad x^2 \leqq 1/9,$$
$$4x^2 = (3y^2 - 1)^2, \qquad 1/9 \leqq x^2 \leqq 1/4.$$

It is interesting to note that the direction of the path of the centroid is parallel to the parametric diameter and therefore that the derivative exists at the four points $(\pm 1/3, \pm 1/3)$ where the parabolas are pieced together.

Also solved by R. G. Albert, E. F. Allen, Ferrel Atkins, Edward Barbeau, Merrill Barnebey, Julian Braun, D. R. Brillinger, E. W. Brown, P. L. Chessin, J. W. Clawson, David Fink, Jose Gallego-Diaz, Michael Goldberg, R. E. Graf, S. H. Greene, J. W. Haake, J. D. Haggard and R. G. Smith (jointly), Corinne Hattan, A. R. Hyde, J. D. E. Konhauser, Morton Kupperman, Peter Landweber, J. H. Leshler and Dale Woods (jointly), Joe Lipman, E. W. Marchand, D. C. B. Marsh, J. B. Muskat, C. S. Ogilvy, P. D. Parker, M. J. Pascual, W. D. Peeples, Jr., L. A. Ringenberg, Jeff Ritterman, D. A. Robinson, Azriel Rosenfeld, Nathan Schwid, Donato Teodoro, C. W. Trigg, S. I. Vrooman, Herbert Wolf, David Zeitlin, and one anonymous solver.

Pascual considered the analogous problem in three space, where the square is replaced by a cube and the diametral line by a diametral plane. Ogilvy proposed the allied problem: What is the locus of the centroid if the arbitrary diameter is fixed and the square is rotated?

An Unusual Differential Equation

E 1303 [1958, 122]. *Proposed by M. J. Hellman, Rutgers University*

Solve the differential equation $dy/dx = \Re(z^n)/\Im(z^n)$, where $z = x + iy$, n is a positive integer, $\Re(z^n)$ denotes the real part of z^n, and $\Im(z^n)$ denotes the imaginary part of z^n.

I. *Solution by J. D. E. Konhauser, Haller, Raymond and Brown, Inc., State College, Pa.* In polar coordinates the differential equation becomes $dr/d\theta = r \tan (n+1)\theta$, the solution of which may be written

$$r^{n+1} \cos (n + 1)\theta = \Re(z^{n+1}) = \text{constant}.$$

II. *Solution by Chih-yi Wang, University of Minnesota.* Since $x = (z+\bar{z})/2$, $y = (z-\bar{z})/2i$, where $\bar{z}$ is the complex conjugate of z, the given differential equa-

tion is reduced at once to $z^n dz+\overline{z^n}\,\overline{dz}=0$. Hence the general solution is $\Re(z^{n+1})$ = constant.

III. *Solution by L. R. Bragg, Duke University.* Noting that $\Im(z^n) = -\Re(iz^n)$, the given equation can be written $\Re[z^n]+\Re[iz^n dy/dx]=0$, or

$$\Re[z^n(1 + i dy/dx)] = 0.$$

This has the solution $\Re[z^{n+1}]$ = constant.

Also solved by J. W. Adams, D. S. Adorno, A. N. Aheart, R. G. Albert, Philip Bacon, J. L. Baker, B. H. Bissinger, Louis Brand, Julian Braun, D. A. Breault, D. R. Brillinger, E. W. Brown, C. N. Campopiano, W. B. Carver, P. L. Chessin, A. G. Clark, A. E. Danese, E. S. Eby and H. F. Illson (jointly), E. L. Ellis and D. L. Muench (jointly), Jose Gallego-Diaz, Michael Goldberg, R. N. Gordon and R. H. Sprague (jointly), S. H. Greene, Corinne Hattan, A. R. Hyde, D. A. Kearns, M. S. Klamkin and D. J. Newman (jointly), Donald Knuth, Morton Kupperman, C. E. Langenhop, L. E. Larson, Joe Lipman, R. L. London, S. Marein-Efrón, D. C. B. Marsh, C. S. Ogilvy, M. J. Pascual, J. L. Pietenpol, B. E. Rhoades, D. A. Robinson, Azriel Rosenfeld, Nathan Schwid, P. W. Shaw, T. H. Slook, O. E. Stanaitis, Donato Teodoro, S. I. Vrooman, R. J. Wagner, Dale Woods, J. W. Young, David Zeitlin, and the proposer.

Alternative expressions for the solution are

$$x\Re(z^n) - y\Im(z^n) = C,$$

$$\sum_{k=0}^{[(n+1)/2]} (-1)^k \binom{n+1}{2k} x^{n-2k+1}y^{2k} = C.$$

Klamkin and Newman gave the generalization: If

$$dy/dx = \Re[f(z)(a - ib)]/\Im[f(z)(a - ib)],$$

then

$$y = a\Re\int f(z)dz + b\Im\int f(z)dz.$$

The given problem is the case where $f(z)=z^n$, $a=1$, $b=0$.

A Property of the Morley Configuration

E 1304 [1958, 122]. *Proposed by W. B. Carver, Cornell University*

Let A_1, A_2, A_3 be the vertices of any triangle and let the arc of the circumcircle from A_i to A_j be trisected by the points T_{ij} and T_{ji}, T_{ij} adjacent to A_i and T_{ji} adjacent to A_j, $i, j=1, 2, 3$. Further, let A_1T_{32} and A_3T_{12} intersect in P_2, A_1T_{23} and A_2T_{13} intersect in P_3. Show that $T_{31}T_{21}$ is parallel to P_2P_3.

Solution by Jose Gallego-Diaz, Vanderbilt University. Let A_3T_{21} and A_2T_{31} intersect in P_1. We know (see, *e.g.*, H. D. Grossman, *The Morley triangle: a new geometric proof*, this MONTHLY [1943, 552]) that $P_1P_2P_3$ is the Morley triangle of $A_1A_2A_3$ and that $\sphericalangle P_3P_2A_1=\pi/3+A_3/3$. But, if Q is the intersection of $T_{21}T_{31}$ with A_1T_{32}, we also have $\sphericalangle T_{21}QA_1=2A_3/3+A_1/3+A_2/3=\pi/3+A_3/3$. It follows that $T_{31}T_{21}$ is parallel to P_2P_3.

Also solved by R. G. Albert, Leon Bankoff, J. W. Clawson, A. R. Hyde, J. D. E. Konhauser, D. C. B. Marsh, and Sister M. Stephanie.

Bankoff gave the reference, V. Thébault, *The triangle*, Scripta Mathematica, vol. 22, 1956, p. 27.

Existence and Construction of a Certain Matrix

E 1305 [1958, 122]. *Proposed by Ky Fan, Oak Ridge National Laboratory*

Given a positive integer n and a symmetric 3×3 matrix $A=(a_{ij})$ with nonnegative integral elements, when does there exist an $n\times3$ matrix B such that $B^*B=A$ (here B^* denotes the transpose of B) and every element of B is either 0 or 1? Describe a method for finding all solutions B.

Solution by the proposer. First observe that if B is a solution, then any matrix obtained from B by a permutation of the rows is also a solution. It is therefore natural to consider two solutions as equivalent if they differ only by a permutation of the rows.

If every element of an $n\times3$ matrix B is 0 or 1, then there are eight possible types of row vectors in B, namely:

$$(1,1,1),\quad (1,1,0),\quad (1,0,1),\quad (0,1,1),$$
$$(1,0,0),\quad (0,1,0),\quad (0,0,1),\quad (0,0,0).$$

Let the numbers of row vectors in B of each of these eight types be denoted by b_{123}, b_{12}, b_{13}, b_{23}, b_1, b_2, b_3, b respectively. These eight numbers are nonnegative integers with sum equal to n, and they determine B up to a permutation of the rows. If $B^*B=A$, then we must have

$$b_{123} \geqq 0, \tag{1}$$

$$b_{12} = a_{12} - b_{123} \geqq 0, \tag{2}$$

$$b_{13} = a_{13} - b_{123} \geqq 0, \tag{3}$$

$$b_{23} = a_{23} - b_{123} \geqq 0, \tag{4}$$

$$b_1 = a_{11} - (a_{12} + a_{13}) + b_{123} \geqq 0, \tag{5}$$

$$b_2 = a_{22} - (a_{12} + a_{23}) + b_{123} \geqq 0, \tag{6}$$

$$b_3 = a_{33} - (a_{13} + a_{23}) + b_{123} \geqq 0, \tag{7}$$

$$b = n - (a_{11} + a_{22} + a_{33}) + (a_{12} + a_{13} + a_{23}) - b_{123} \geqq 0. \tag{8}$$

This can easily be seen if we regard B as the incidence matrix of three subsets S_1, S_2, S_3 of the set $\{1, \cdots, n\}$. (Then a_{ij} is the number of elements of $S_i \cap S_j$; b_1 is the number of those elements which belong to S_1 and only to S_1; b_{12} is the number of those elements which belong to S_1, S_2, but not to S_3; *etc.*)

Let p denote the least of the four integers

$$a_{12},\ a_{13},\ a_{23},\ n - (a_{11} + a_{22} + a_{33}) + (a_{12} + a_{13} + a_{23}),$$

and let q denote the greatest of the four integers

$$0,\ (a_{12} + a_{13}) - a_{11},\ (a_{12} + a_{23}) - a_{22},\ (a_{13} + a_{23}) - a_{33}.$$

Then inequalities (1)–(8) imply

$$p \geqq q. \tag{9}$$

Therefore inequality (9) is a necessary condition for B to exist.

This necessary condition (9) is also sufficient. In fact, when (9) is fulfilled, we can choose an integer b_{123} satisfying all inequalities (1)–(8). There are $p-q+1$ possible choices for b_{123}, since it can be taken to be any one of the integers $q, q+1, \cdots, p-1, p$. After having chosen b_{123}, the nonnegative integers b_{12}, b_{13}, b_{23}, b_1, b_2, b_3, b are determined by the equations (2)–(8), and we have

$$b_{123} + b_{12} + b_{13} + b_{23} + b_1 + b_2 + b_3 + b = n.$$

Then any $n \times 3$ matrix B with these preassigned numbers b_{123}, b_{12}, $\cdots$, b_3, b of rows of each of the eight types will satisfy $B^*B = A$. Since there are $p-q+1$ possible choices for b_{123}, the total number of nonequivalent solutions B is $p-q+1$.

Remark 1. The necessary and sufficient condition (9) can be written as follows:

$$a_{ii} - a_{ij} \geqq 0, \qquad (i \neq j), \tag{9.1}$$

$$n - (a_{ii} + a_{jj}) + a_{ij} \geqq 0, \qquad (i \neq j), \tag{9.2}$$

$$a_{ii} - (a_{ij} + a_{ik}) + a_{jk} \geqq 0, \qquad (i, j, k \text{ all distinct}), \tag{9.3}$$

$$n - (a_{11} + a_{22} + a_{33}) + (a_{12} + a_{13} + a_{23}) \geqq 0. \tag{9.4}$$

Remark 2. The same problem for a symmetric 4×4 matrix A is surprisingly difficult. No necessary and sufficient condition is known.

Also solved by D. A. Breault, D. R. Brillinger, A. S. Davis, S. H. Greene, J. W. Haake, Joe Lipman, D. C. B. Marsh, and D. A. Robinson.

The following examples were given by Marsh. Consider the three matrices

$$A_1 = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

If $A = A_1$, there is no solution; if $A = A_2$, there is essentially only one solution provided $n > 6$; if $A = A_3$, there are two and only two nonequivalent solutions provided $n > 4$.

ADVANCED PROBLEMS AND SOLUTIONS

EDITED BY E. P. STARKE, Rutgers University

Send all communications concerning Advanced Problems and Solutions to E. P. Starke, Rutgers University, New Brunswick, New Jersey. All manuscript should be typewritten, with double spacing and margins at least one inch wide. Problems containing results believed to be new or extensions of old results are especially sought. Proposers of problems should also enclose any solutions or information that will assist the editor. In general, problems in well-known textbooks or results in readily accessible sources should not be proposed for this department.

PROBLEMS FOR SOLUTION

4804. *Proposed by I. S. Gâl, Cornell University*

A theorem of Baire states that every lower semi-continuous function on a metric space is the pointwise limit of an increasing sequence of continuous functions. Show by an example that the theorem cannot be extended to arbitrary uniform spaces.

4805. *Proposed by R. R. Goldberg, Pittsburgh, Penna.*

The following relation is found to be true for $n=1, 2, \cdots, 6$.

$$n^2 \sum_{k=0}^{n} \frac{(-1)^{n+k}}{(n-k)!} \frac{(n+k-1)!}{k!k!} \sum_{j=1}^{n+k-1} \frac{1}{j} = 1.$$

Is it true for all positive integers n?

4806. *Proposed by D. J. Newman, AVCO Research and Development, Lawrence, Mass.*

Let $0=a_0<a_1<a_2<\cdots$ be integers. Prove that $\sum_{n=0}^{\infty} z^{a_n}$ has no zeros in $|z|<(\sqrt{5}-1)/2$. Also, this is the best possible constant.

4807. *Proposed by Victor Thébault, Tennie, Sarthe, France*

Determine the integral solutions of the equation

$$(m-1)x^2 + my^2 = (m+1)z^2.$$

4808. *Proposed by J. M. Gandhi, Jain Engineering College, Panchkoola, India*

Consider the expression $S_2(n, i) = \sum a_1^2 a_2^2 \cdots a_i^2$, where the sum is taken over all possible integral choices of the a's such that $1 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_i \leqq n$. Prove that

$$2(2^{2n}-1)B_{2n} = (-1)^{n-1}\{(n-1)!^2 - (n-2)!^2 S_2(n-2, 1) + (n-3)!^2 S_2(n-3, 2) - \cdots + (-1)^n 1!^2 S_2(1, n)\},$$

where the B_{2n} are the well-known Bernoulli numbers.

4809. *Proposed by Sylvan H. Greene, General Electric Co., Philadelphia*

Let n be an odd, square-free integer greater than 3; let A_n be the set of all

$a \pmod n$ such that $(a/n) = +1$, and B_n that of all $b \pmod b$ such that $(b/n) = -1$, where (c/n) is the Jacobi symbol. Prove that in a complete system of residues (mod n), $\sum a \equiv \sum b \equiv 0 \pmod n$. The summations are taken over all elements of A_n and B_n respectively.

SOLUTIONS

Power Sums of Roots

4758 [1957, 676]. *Proposed by Leonard Carlitz, Duke University*

Let $x_1, \cdots, x_n$ denote the roots of

$$(x - a + \sqrt{1 - 2ax + x^2})^n + (x - a - \sqrt{1 - 2ax + x^2})^n = 2(a^2 - 1)^{n/2}.$$

Evaluate the power sums $\sigma_k = x_1^k + \cdots + x_n^k$ $(0 \leq k < n)$.

Solution by W. A. Al-Salam, Duke University. Consider the polynomial

$$P(x) = (x - a + \sqrt{1 - 2ax + x^2})^n + (x - a - \sqrt{1 - 2ax + x^2})^n - 2(a^2 - 1)^{n/2}.$$

On one hand we have, for large values of x,

$$\frac{P'(x)}{P(x)} = \sum_{k=1}^{n} \frac{1}{x - x_k} = \sum_{r=0}^{\infty} \frac{\sigma_r}{x^{r+1}}. \tag{1}$$

On the other hand from the definition of $P(x)$

$$\begin{aligned} &\frac{P'(x)}{P(x)} \\ &= \frac{n}{\sqrt{1 - 2ax + x^2}} \cdot \frac{(x - a + \sqrt{1 - 2ax + x^2})^n - (x - a - \sqrt{1 - 2ax + x^2})^n}{P(x)} \\ &= \frac{n}{\sqrt{1 - 2ax + x^2}} - \frac{2n}{\sqrt{1 - 2ax + x^2}} \\ &\quad \cdot \frac{(x - a - \sqrt{1 - 2ax + x^2})^n - (a^2 - 1)^{n/2}}{P(x)}. \end{aligned}$$

We note that the first term in the right hand side of (2) is the generating function for $P_r(a)$, the Legendre polynomials, and for large values of x gives

$$\frac{n}{\sqrt{1 - 2ax + x^2}} = n \sum_{r=0}^{\infty} \frac{P_r(a)}{x^{r+1}}.$$

Now

$$\frac{(x - a + \sqrt{1 - 2ax + x^2})^n - (a^2 - 1)^{n/2}}{(x - a - \sqrt{1 - 2ax + x^2})^n - (a^2 - 1)^{n/2}} = -\left(\frac{x - a + \sqrt{1 - 2ax + x^2}}{x - a - \sqrt{1 - 2ax + x^2}}\right)^{n/2}$$

$$= -\left(1 + \frac{2}{a^2 - 1}\cdot(x^2 - 2ax + 1) + \frac{2(x - a)}{a^2 - 1}\sqrt{1 - 2ax + x^2}\right)^{n/2}.$$

Thus for large values of x we can see by easy calculation that the second term in the right hand side of (2) has a development in which all the powers of $1/x$ are $\geqq n$. Hence, comparing (1) and (2), we get $\sigma_r = nP_r(a)$, $(0 \leqq r < n)$.

Also solved by Emil Grosswald, Peter Henrici, M. S. Klamkin, D. C. B. Marsh, F. D. Parker, Blagovest Sendov, G. Szegö, Chih-yi Wang, and the proposer.

Nonuniform Convergence

4760 [1957, 676]. *Proposed by G. U. Brauer, University of Minnesota*

Let $f(x)$ be a real function such that $f(0) = 0$, $f(1) \neq 0$, $\lim_{n\to\infty} f(n) = 0$, where n takes on positive integral values. Construct a sequence of integers $\{a_n\}$, $a_n \to \infty$ as $n \to \infty$, and a compact set C such that $f(a_n x) \to 0$ nonuniformly for x in C.

Solution by Hans Schneider, The Queen's University, Belfast, Ireland. Let C be the compact set consisting of 0 and all rationals of the form $1/n$, where n is a positive integer. Set $a_n = n!$. For each nonzero x in C it is clear that $a_n x$ is an integer for all sufficiently large n and that $\lim_{n\to\infty} a_n x = \infty$. Hence $\lim_{n\to\infty} f(a_n x) = 0$ for all x in C.

Now let $0 < \epsilon < |f(1)|$. Then, for each positive integer n, we have the inequality $|f(a_n x)| = |f(1)| > \epsilon$ if $x = 1/n!$, and therefore the convergence is nonuniform on C.

Also solved by Montford Plebstnoch, R. L. Plunket, Blagovest Sendov, and the proposer.

A Summation Related to No. 4592

4762 [1957, 676]. *Proposed by Samuel Beatty, University of Toronto*

Define γ_i by the relations

$$\sum_{r=1}^{n} \frac{\log^i r}{r} = \int_1^n \frac{\log^i x}{x}\,dx + \gamma_i + o(1).$$

Show that

$$\sum_{r=1}^{\infty} (-1)^{r+1} \frac{\log^p r}{r} = \frac{\lambda^{p+1}}{p+1} - \left[\lambda^p \gamma + \binom{p}{1}\lambda^{p-1}\gamma_1 + \cdots + \binom{p}{p-1}\lambda\gamma_{p-1}\right],$$

$(p = 2, 3, \cdots)$, where $\lambda = \log 2$ and γ is Euler's constant. This is a generalization of no. 4592 [1954, 350].

Editorial Note. It was overlooked that a solution of the current problem appears, culminating in equation (8), in *The Power Series Coefficients of* $\zeta(s)$, by Briggs and Chowla, this MONTHLY, vol. 62, 1955, pp. 323–325. This paper is referred to in the solution of Problem 4592 which appears in the October, 1955 issue and, as a matter of fact, it was this problem which instigated the paper.

Solutions submitted by W. A. Al-Salam, W. E. Briggs, R. G. Buschman, L. Carlitz, Lawrence Glasser, Emil Grosswald, M. S. Klamkin, Bryant Tuckerman and Tien Chi Chen, Chih-yi Wang, David Zeitlin, and the proposer.

A Minimax Problem

4763 [1957, 746]. *Proposed by Ky Fan, Oak Ridge National Laboratory*

For n positive numbers x_i, let $f(x_1, \cdots, x_n)$ and $g(x_1, \cdots, x_n)$ denote respectively the least and the greatest of the $n+1$ quantities

$$x_1, \frac{1}{x_1} + x_2, \cdots, \frac{1}{x_{n-1}} + x_n, \frac{1}{x_n}. \tag{1}$$

Prove that

$$\operatorname*{Max}_{x_i>0} f(x_1, \cdots, x_n) = \operatorname*{Min}_{x_i>0} g(x_1, \cdots, x_n) = 2\cos\frac{\pi}{n+2}. \tag{2}$$

Solution by D. S. Greenstein, University of Michigan. Assume that u is a positive real such that

$$u = x_1 = \frac{1}{x_1} + x_2 = \cdots = \frac{1}{x_{n-1}} + x_n = \frac{1}{x_n}. \tag{3}$$

Then $u = \max f = \min g$ for all choices of x_i. For, to increase f we would have to increase x_1, which would necessitate increasing x_2, *etc.*, finally necessitating an increase of x_n, which would decrease $1/x_n$ and decrease f. A similar argument applies to decreasing g.

From (3) we see that $x_1 > \cdots > x_n$. Further, $x_1 < 2$ since $x_1 \geqq 2$ implies $x_n > 1$ contrary to $x_n = 1/x_1$. We may therefore put $u = 2\cos\theta$. For (3) to hold, we must have $x_1 = u$, $x_2 = u - 1/u$, $x_3 = u - 1/(u - 1/u)$, *etc.*, which may be rewritten $x_k = Q_k(u)/Q_{k-1}(u)$, $(k = 1, \cdots, n)$, where the Q_k are defined by

$$Q_0 = 1,\ Q_1 = u,\ Q_{k+1} = uQ_k - Q_{k-1}. \tag{4}$$

Since $1/x_n = u$, we must have $u = Q_{n-1}(u)/Q_n(u)$, which is equivalent to $Q_{n+1}(u) = 0$. From $u = 2\cos\theta$ it is easily verified that the unique solution of (4) is given by $Q_k = \sin(k+1)\theta/\sin\theta$. Hence θ is a multiple of $\pi/(n+2)$. But $Q_1, \cdots, Q_n$ all positive require $\theta = \pi/(n+2)$. Finally $u = 2\cos(\pi/(n+2))$ as required.

Also solved by Ward Cheney and Allan Goldstein, Emil Grosswald, D. C. B. Marsh, M. F. Neuts, Roly Rasmussen, G. Szegö, R. S. Varga, Chih-yi Wang, and the proposer.

A Limit of a Sum

4764 [1957, 737]. *Proposed by A. E. Currier, U. S. Naval Academy*

Prove

$$\lim_{n\to\infty} \sum_{j=0}^{n} \binom{2n-j}{n} (-4)^j \Big/ \binom{2n}{n} = \frac{1}{3}.$$

Solution by D. G. Cantor, University of California, Los Angeles. Let

$$f_n(x) = \binom{2n}{n}^{-1} \sum_{j=0}^{n} \binom{2n-j}{n} x^j.$$

By direct substitution one may verify that

$$2(x-1)f_n(x) = x - 2 + x^2(n/(2n-1)) \cdot f_{n-1}(x),$$

and by induction show that, for $x \neq 1$,

$$f_n(x) = \frac{x-2}{2x-2} \sum_{k=1}^{n} \prod_{i=k}^{n-1} \left(\frac{x^2}{4(x-1)} \cdot \frac{2i+2}{2i+1} \right) + \prod_{i=0}^{n-1} \left(\frac{x^2}{4(x-1)} \cdot \frac{2i+2}{2i+1} \right).$$

Clearly the sequence $\{f_n(x)\}$ converges when $|x^2/4(x-1)| < 1$, *i.e.*, when $-2-2\sqrt{2} < x < -2+2\sqrt{2}$, by comparison with the geometric series. Then $f(x) = \lim_{n\to\infty} f_n(x)$ exists and

$$2(x-1)f(x) = x - 2 + x^2(1/2)f(x),$$

whence $f(x) = 2/(2-x)$, and $f(-4) = 1/3$ as required.

Also solved by M. T. Bird, D. C. B. Marsh, Yoshio Matsuoka, G. Szegö, and the proposer.

Editorial Note. By a somewhat extended analysis, Szegö shows that, for $n \to \infty$,

$$f_n(x) \to (1 - x/2)^{-1}, \qquad -2 - 2\sqrt{2} < x < 2;$$

$$f_n(x) \cong \frac{x}{x-1} \cdot \left(\frac{x^2}{4(x-1)} \right)^n \cdot \sqrt{\pi n}, \qquad x \geqq 2 \text{ or } x \leqq -2 - 2\sqrt{2}.$$

Continuous Increasing Function

4765 [1957, 746]. *Proposed by J. L. Massera, Instituto de Matematica y Estadistica, Montevideo, Uruguay*

Let $f(x)$ be a real function defined for $x \geqq 0$. If (i) f has a finite upper bound in any finite interval, and (ii) there are two positive numbers h, k such that $x' - x'' \geqq h$ implies $f(x') - f(x'') \geqq k$, then there is an increasing function $g(x)$ having as many continuous derivatives as we please, such that $g(x-h) < f(x) < g(x)$ for all sufficiently large x.

Discussion by J. L. Pietenpol, Columbia University. A stronger hypothesis is called for. As it stands, the theorem is false, as an example will show: Let $f(x) = 3[x] - x$, $h = k = 1$, where $[x]$ is the greatest integer function. The conditions of the problem are met. We now seek an increasing function $g(x)$ such that $g(x-1) < f(x) < g(x)$, which is equivalent to $f(x) < g(x) < f(x+1)$, for sufficiently large x. But it is clear that any $g(x)$ which satisfies this condition is necessarily discontinuous at all integral values of x.

RECENT PUBLICATIONS

EDITED BY RICHARD V. ANDREE, University of Oklahoma

All books for review should be sent directly to R. V. Andree, Department of Mathematics, University of Oklahoma, Norman, Oklahoma, and not to any of the other editors or officers of the Association.

Consiglio Nazionale dell Ricerche Monografie Matematiche. Vol. 4. *Calcolo dell Matrici.* By Salvatore Cherubino. Edizioni Cremonese, Rome, 1957. vi+322 pp.

The reviewer read this book with a great deal of pleasure because it is different from most of the books on matrices which are currently appearing. While the concept of vector space is introduced, it is not used very much. The reduction to canonical form under similarity transformations is limited to the field of the characteristic roots. A paragraph entitled "the concepts of abstract algebra" consists essentially of the derivation of the first and second regular representations of a finite linear associative algebra. The concepts of ring and field are introduced, but most of the book is concerned with matrices with either real or complex elements.

There is really a lot of factual material in this book, much of it not readily accessible in textbooks. The chapters dealing with the characteristic roots are especially complete, treating approximation to the dominant root, Hurwitz' stability theorem, maxima and minima of quadratic forms, Borchardt's theorem, bounds for the roots, *etc.* But the author's principal interest seems to be in the differentiation and integration of matrices whose elements are functions of one or more independent variables. Even the Cayley-Hamilton theorem is proved by a power series expansion.

Coverage and references are international, with Italian authors getting only a shade the best of it. Classical theorems seem to be attributed to the proper authors. There are many minor turns and points of view which the reviewer has not encountered elsewhere. The paper and printing are excellent, and so is the cover.

C. C. MACDUFFEE
University of Wisconsin

Flachenverbiegung im Grossen. By N. W. Efimow. Akademie-Verlag, Berlin, 1957. xi+233 pp. DM 35.50 (about $8.50).

The book consists of two parts: the first, ending at page 112, is a translation of Efimow's report (Uspehi 1948) on *Qualitative questions in the theory of deformations of surfaces*; the second, pp. 113–230, by E. Rembs and K. P. Grotemeyer, consists of notes referring to topics of the first part and containing mostly results discovered after 1948, frequently answers to problems raised in the first part.

Efimow's report is a very clear exposition which can be read and enjoyed

also by the nonspecialist. The notes, while individually well written, are by their very nature incoherent and cannot be read as a book. However, they provide a great deal of valuable information to the specialist.

In both parts the longer proofs are only briefly sketched. This permits the authors to include a wealth of material. Consequently we must limit ourselves here to indicating a few of the main themes.

(1) The existence and uniqueness of the realizations as convex surfaces of metrics with nonnegative curvature. The classical methods of Weyl, Lewy, Cohn-Vossen, Herglotz are discussed, but the emphasis, at least for realization problems, lies on the modern methods developed by A. D. Alexandrov and Pogorelov.

(2) Deformations in the large of convex surfaces mainly by means of Alexandrov's Gluing Theorem. Part 2 gives many explicit deformations of special surfaces.

(3) Deformations in the small of, not necessarily convex, smooth surfaces, in particular Efimow's results on nondeformable surfaces with flat points.

(4) A general theory of infinitesimal deformations of the first and higher orders. The rigidity of special surfaces like surfaces with positive curvature, closed or with boundaries and sometimes boundary conditions, of tori, and (in a modified sense) of convex polyhedra. The second part emphasizes, in particular, the integral formulae entering this theory.

A very extensive list of references and a subject index conclude the book.

H. Busemann
University of Southern California

Plane Trigonometry. By Frank A. Rickey and J. P. Cole. Holt, New York, 1958. x+260 pp. $3.25.

This book gives an excellent analytic treatment of its subject. At the same time it presents with sufficient detail and applications the solution of right and general triangles. It treats the usual topics,—trigonometric functions of angles measured in degrees and radians, evaluation of trigonometric functions of special angles, use of tables of trigonometric functions, graphs of trigonometric functions, solution of triangles, trigonometric identities, solution of equations, inverse trigonometric functions,—and includes graphs in polar coordinates and a chapter on complex numbers. The appendix discusses accuracy of approximate numbers and contains a square- and cube-root table and four-place tables of natural functions and of logarithms of numbers and trigonometric functions. Answers to the odd-numbered problems are given.

Throughout the book the authors stress derivation of formulas rather than formula memorization. They succeed in making the general proofs of theorems clear and accurate; the addition formulas are proved by direct application of the distance formula in cartesian geometry. Trigonometric graphs are introduced early; possibly they are overworked as a visual aid in solving trigonometric equations. Exercises are carefully selected to take care of necessary drill and to

train the student in analytic methods. As a quite natural part of the subject of plane trigonometry the authors present concepts and topics useful in more advanced mathematics, for example, trigonometric functions of a number, principal values of inverse trigonometric functions, the function $(\sin x)/x$ when x is small, polar coordinates, complex numbers.

This trigonometry is a welcome addition to the textbooks which emphasize an analytical approach to the subject.

HELEN G. RUSSELL
Wellesley College

Calculus With Analytic Geometry. By R. E. Johnson and F. L. Kiokemeister. Allyn and Bacon, Boston, 1957. xi+650 pp. $7.95.

It is common for "*A*-students" in a "standard" calculus course to remark to the effect: "I can work all of the problems but I don't understand it!" This book goes a long way toward all that a textbook can do now for such students. (It is necessarily a compromise between the here-is-how-you-do-it-and-never-mind-why type of text and a course in real variables.) It is an impressive job of exposition with a fair amount of modern terminology and a considerable amount of mathematical care. It has plenty to challenge bright students and would not need to be fatal to average students.

Miscellaneous notes for flavor: Functions are named by single letters—f is the function whose value at x is $f(x)$. The phrase "if and only if" is used without blush. Absolute value and inequality symbols are used freely. Limits are hit heavily. The greatest integer function and other "unusual" functions are used to give interesting examples and problems and to show that not all functions are everywhere continuous. The tangent to a curve is treated with more than usual rigor. Physicists will like the distinction between "speed" and "velocity." The notion of open and closed intervals is used throughout. A region bounded by a curve is *defined* to have an area given by an integral and the common "proof" by witchcraft is omitted. (The additivity of area and its lineage from polygons is effectively hinted at.) L.U.B. and G.L.B. are introduced on page 197 in preparation for defining an upper integral and a lower integral for a function over a given domain.

A striking feature of the book is the frequent correspondence between concise, technical language and an easygoing interpretation of it. After three equivalent definitions of continuity (in hope that one will strike home) and three pages of examples and explanation we find the familiar: "Roughly speaking if a function f is continuous in an interval $[a, b]$, the graph of f between $x=a$ and $x=b$ has no jumps in it. This piece of the graph of f may be sketched without lifting the pencil from the paper" (p. 76).

Although this book contains a rather complete introduction, it is a rare student who will be able to cover the introduction at the implied pace. Either the first ninety pages will have to be taken slowly or students with strong high school backgrounds will be required. However, as implied by the title, analytic

geometry is not a prerequisite. Enough analytic geometry is contained in the first ninety pages to make differentiation of polynomials understandable. After polynomial differentiation and its applications are well established, this knowledge is turned back onto an efficient treatment of "Conic Sections and Other Algebraic Curves." Analytic geometry is therefore effectively intermixed with calculus to make both subjects more understandable and interesting.

There are some flaws. For example, the authors are not sure whether to call angles or line segments of the same measure congruent or equal; they try it both ways. Rarely, nonsense creeps in: "A collection of points satisfying some geometric condition is called a locus" (p. 27). Then certainly every set of points is a locus and the new term is superfluous. The treatment of coordinates on a line on page 11 is confusing. Differentials are as slippery as ever. This list could be much extended. Toward the end of the book it runs downhill toward the usual agglomeration of mysterious topics.

A principal objection is that it is not reformed enough. The word "set" is painfully avoided until page 196. The language and intuition of set theory should be used throughout. Functions should be sets of ordered pairs of numbers (with the single-valued condition). Sequences should be functions over the positive integers. $\sum$-notation should be introduced earlier. And so on. The only trouble is that by the time all such changes were made it would be an extremely demanding task to prepare a text as useful in the classroom as this one.

D. A. PAGE
University of Illinois

The Numerical Solution of Two-Point Boundary Problems in Ordinary Differential Equations. By L. Fox. Oxford University Press, 1957. xi+371 pp. $9.60.

This book deals with differential equations having the extra conditions imposed for more than one value of the independent variable. It serves a very useful purpose, since most numerical techniques are set for one point initial conditions.

A great deal of the work being done in this country with numerical methods is, however, done in and around large computers. One must be warned, therefore, that while almost every technique introduced by the author can be adapted to a large computer, there is often a difficult choice as to which technique to use. Again, this is not the fault of the author, for this book is aimed at the competent computer, not the competent machine programmer. Let the latter be warned by the quotation from Chapter 6, "The choice of method depends solely on the structure of the equation and computational convenience."

The first two chapters are devoted to notation and derivation of formulae. Chapter three supplies the necessary algebraic techniques for solving the simultaneous equations that will continually appear. Succeeding chapters then treat second-order, first-order, and higher-order problems. It might be thought that first-order problems hardly belong, but their solution is peculiarly amenable to second-order techniques by introducing an artificial boundary value.

Eigenvalue problems are well cared for, starting with a useful description of methods of finding eigenvalues. Cases are included where one of the boundary values is infinite. A chapter describing initial value methods points out the differences from other methods.

All too frequently books on numerical methods do not emphasize accuracy enough, but in this case an entire chapter studies the subject thoroughly. If one tries to sum up quite briefly, here is a book which covers its problem in very great detail, with a tremendous number of examples worked out, so that any reasonably interested person may learn a great deal of useful information. It is not a reference book in that without knowing most of the material it is not possible to make a reasonable choice of method of attack. It belongs in the library of anyone seriously interested in such problems, and it should be available to any large-machine computing group.

R. G. SELFRIDGE
U. S. Naval Ordnance Test Station

Queues, Inventories and Maintenance. By Philip M. Morse. Wiley, New York, 1957. ix+202 pages. $6.50.

This volume is the first in a series of monographs published by Operations Research Society and the editors are certainly to be congratulated for having made an ideal initial choice.

The author, one of the pioneers in the field of Operations Research, has taken a problem area of great analytic interest and practical significance, the problem of queuing, and discussed various aspects of it in a very lucid fashion.

What is particularly attractive about this book is the clear and leisurely fashion in which concepts are introduced, problems are posed and equations are treated. The author is clearly not ashamed to use the English language rather than symbols to make his points, an attitude which, unfortunately, is not shared by a large number of writers of current research articles and books.

The general problem is that of servicing objects which arrive at a facility, wait until attended to, and then depart. The question is that of determining the departure rate from the arrival rate, the servicing rate and the structure of the facility. Examples of systems of this nature are furnished by telephone exchanges, department stores, airfields, hospital clinics, production lines, and automobile traffic.

The author explains how to consider these problems in terms of a probabilistic model, and how this model may be used to treat a number of interesting situations, corresponding to different assumptions concerning arrival time and the structure of the facility.

The last two chapters are devoted to some applications of these techniques to inventory control and maintenance of equipment. Here it might be well to add to the references given by the author those treating these questions by means of a different technique, that of dynamic programming; *cf.* Arrow, Harris

and Marschak, *Optimal Inventory Policy*, Econometrica, 1951; Dvoretzky, Kiefer and Wolfowitz, *The Inventory Problem*, I, II, Econometrica, 1952; and Bellman, *Dynamic Programming*, Princeton University Press, 1957, where other references may be found.

The author appends a sizable number of references he has found useful in writing the book, and refers to other sources which contain extensive bibliographies of these topics.

This volume is highly recommended either as textbook or as collateral reading in a course on Operations Research, Mathematical Economics, or Applied Probability Theory. Even if the reader is not interested in queues, *per se*, he will find both the detailed discussion of model-building and the mathematical analysis extremely valuable.

RICHARD BELLMAN
The RAND Corporation

Integrated Algebra and Trigonometry. By Robert C. Fisher and Allen D. Ziebur. Prentice-Hall, New Jersey, 1958. 427 pp. $7.95.

It is the novel way of treating many familiar topics which makes this work a stimulating one to read. The concept which unites the many topics in this book is that of function, a relationship between two sets of numbers. More emphasis is placed on inequalities and absolute values than is customary in the usual text on algebra. Trigonometric functions are introduced via a trigonometric point on a unit circle (essentially radian measure) and all the properties of these functions, such as periodicity, variation, addition formulae and evenness or oddness are developed without any reference to the traditional definitions using right triangles.

The factoring of quadratic trinomials is relegated to a position after the solution of quadratic equations, and hence the relation between the factors and the roots of the associated quadratic equation is apparent. Systems of simultaneous linear equations are solved by reducing them to a canonical triangular system. With this approach, the concepts of the matrices associated with such systems and their properties are easily presented. Determinants then appear as numbers associated with square matrices.

Throughout the text the material is excellently presented, and the aim of the authors seems to be to stress ideas rather than the mechanical aspects of the subject. As a result, computational problems and long lists of drill exercises are omitted, and the few tables are abbreviated and poorly labeled. Much of the work is rigorously presented, yet intuitional proofs are given when expedient.

This is a text which should prove stimulating to capable students interested in mathematics and to teachers who are willing to deviate from the traditional methods used in teaching trigonometry and algebra.

R. G. SANGER
Kansas State College

Raum und Gegenraum. Einführung in die neuere Geometrie. By Louis Locher-Ernst. Philosophisch-Anthroposophischer Verlag am Goetheanum, Dornach, Switzerland, 1957. $6.50.

The center of the author's attention is occupied by the principle of duality. The usual way in which this basic idea is presented to novices in the study of projective geometry is fragmentary and unconvincing. The author undertakes not only to remedy this situation, but to work out a complete dual for metrical geometry. He goes about his task with skill and imagination, backed by a consumate art of exposition, aided by an abundance of excellent drawings. The results obtained are applied to some extent to the study of plane curves.

But the real aim of this discussion, in fact the "raison d'être" of the book as a whole, transcends the field of geometry. The principle of duality, which emerged from projective geometry during the first half of the 19th century, put alongside the accustomed point-space a new "plane-space" or "counter-space" ("Gegenraum") which, in the hands of the geometers, became a powerful tool. Furthermore, the principle of duality exerted a great influence upon mathematical philosophy in general, and upon the axiomatic method in particular. To a geometer of the stature of Michel Chasles (1793–1880), this did not exhaust the potentialities of this principle. He perceived that plane-space was destined to play an important role in the study of the physical sciences, and others [*Aperçu historique sur l'origine et le développement des méthodes en géométrie*, first ed., 1837, p. 408]. Towards the end of the first quarter of the present century this idea found adherents in some quarters (see pp. 207 ff). Locher-Ernst's elaboration of the "plane-space" is intended to facilitate the use of that space, rather than the point-space, as a frame of reference by the physicists, biologists, *etc.*

Such a suggestion could not be made at a more appropriate time than the present, when mathematical thinking is predominantly oriented toward applications. Nevertheless, to think of space in terms of planes remains a big order. Be that as it may, students and especially teachers of projective geometry will read Locher-Ernst's work with much profit. The book contains more than two hundred first-rate figures, an interesting preface, a brief table of contents, and no index of any kind.

NATHAN ALTSHILLER COURT
University of Oklahoma

Integral Equations. By S. G. Mikhlin. Pergamon Press, New York, Los Angeles, 1957. xii+338 pp. $12.50.

This book is very elegantly written, and the translator has done an excellent job of retaining its simplicity of style. Part I, of two parts, deals with methods of solution of integral equations, and introduces the reader gradually and smoothly to all the notions required for a complete treatment of the subject at an elementary level. Each topic is illustrated by example, with a practical

view in mind of actually obtaining numerical estimates and solutions. Many classical proofs of some complexity are given in much simplified form.

Even though it is necessary to use the notions of the Lebesgue integral, and mean convergence in many proofs, the presentation is simple enough that a reader without these mathematical disciplines can still follow the proofs, and need only accept the existence of certain integrals. Apart from this, the book is admirably suited as a text in a first course in integral equations, and the wealth of examples and applications (mostly in two dimensions) is sufficient to appeal to nearly all applied interests.

Part I includes the Fredholm theory for the equation of the second kind, including systems, for Volterra, degenerate, and weakly singular kernels; the Hilbert-Schmidt theory of symmetric kernels, and selected examples of singular equations with Hilbert and Cauchy type kernels. Part II gives applications of these integral equations to many problems in two and three dimensions, including Dirichlet's problem, Neumann's problem, and related examples, the biharmonic equation, and numerous problems from hydrodynamics, elasticity theory, and conformal mapping.

GORDON LATTA
Stanford University

Elements of Mathematics. By J. Houston Banks. Allyn and Bacon, Boston, 1956. x+422 pp. $5.75.

This book could be used as a text or reference in a variety of courses. No prerequisite other than elementary arithmetic is necessary, but some previous experience with algebra and geometry would be very desirable. The chapters are, with exceptions noted by the author, independent, and starred sections can be omitted without affecting continuity. Topics currently much discussed, particularly in the fields of elementary and secondary education, are numerous. For examples: the number system, mathematical proof, groups, fields, sets, Boolean algebra, functions and statistics. Some further idea of the wide range of this text may be obtained by noting a few selected topics: bases other than ten, algorithms, indirect proof, Zeno's paradoxes, transfinite numbers and systems of measurement. The logical development of the arithmetic of the natural numbers should be of interest and value to elementary teachers. The chapters on algebra and mathematical proof should be of particular interest to secondary teachers. The text is clearly written but may be somewhat concise for use as a text for prospective and in-service teachers—a use for which it seems otherwise well suited. At times the limited coverage of some topics should be sufficiently stimulating to prompt the student to seek further information. This is not an easy book for backward students but a careful presentation "designed to make more meaingful the fundamental concepts and techniques of mathematics." It serves this purpose well.

JAMES L. SIMPSON
Montana State College

Lie Groups. By P. M. Cohn. Cambridge University Press, 1957, vi+164 pp. $4.00 (Cambridge Tracts in Mathematics and Mathematical Physics, No. 46).

This monograph is intended, as the author mentioned in the preface, to develop the beginning of the theory of Lie groups, especially the fundamental theorems of Lie relating the group to its Lie algebra. The approach is somewhat standard. Nevertheless the author presents the material in a very clear and self-contained manner. Only the most elementary knowledge of groups, vector spaces and general topology is assumed. Among the propositions and definitions, there are illuminating remarks giving the motivation of the concepts and theorems. The organization is good, and the style is so lucid that it can serve as an excellent introduction to the theory of Lie groups.

Chapter I introduces the concepts of analytic manifolds, infinitesimal transformations and differential forms. Chapter II opens with some elementary properties of topological groups; Lie groups and their analytic subgroups are then defined. In Chapter III, the Lie algebra of a Lie group is introduced by means of right infinitesimal translations. One-parameter subgroups and exponential mapping are discussed. Chapter IV deals with the exterior algebra of differential forms. By applying it to Lie groups, the equations of Maurer-Cartan are established.

Chapter V is concerned with the converse of the fundamental theorems of Lie. The author gives, in detail, the proof of the 1-1 correspondence between local Lie groups and their Lie algebras. Chapter VI covers canonical charts (coordinate systems), continuous homomorphisms, quotient Lie groups, the relation between analytic subgroups and Lie subalgebras, and the adjoint representation. In Chapter VII, the author constructs the universal covering group of a Lie group and proves the uniqueness theorem. The book concludes with an appendix on completely integrable system of total differential equations (Frobenius Theorem).

The classification problem and global properties of the underlying space of Lie groups are not touched.

H. C. WANG
Northwestern University

The Analysis of Multiple Time-Series. By M. H. Quenouille. Hafner, New York, 1957. 105 pp. $4.75.

In a series of papers published in the 1920's, G. U. Yule discussed the difficulties encountered when regression or correlation analysis is applied to time-series and the impossibility of interpreting the correlations between time-series without reference to the internal structure of the series. This led to a more intensive study of the manner in which time-series may be generated. Led by Yule, statisticians began to pay more attention to the problems of recognizing, testing, and estimating the structure of time-series.

Because of the complex analysis involved, much of the work has dealt with the analysis of individual time-series although the need for studying multiple time-series is quite apparent, particularly in the field of economics. Numerous papers on various aspects of the analysis of multiple time-series have appeared in the literature from time to time but there remain numerous gaps both in theory and applications.

The author states that his purpose in writing this monograph is to fill some of the gaps and to present a unified account of the methods available for the analysis of multiple time-series.

The manner in which the author has woven together the various aspects of the theory is indicated by the chapter headings: (1) Introduction; (2) Specification; (3) Identification; (4) Preliminary Investigation; (5) Practical Complications; (5) Estimation; (7) Significance and Goodness-of-fit Tests; (8) Practical Examples.

The author has done a remarkably good job on a difficult task. Here is a summary of one approach to the problems of analyzing multiple time-series. The work is concise, at times almost too much so, and is generously illustrated with numerical examples. Shortcomings and gaps remaining in the theory are pointed out rather than suppressed. The printing is good and, except for a few lost decimal points, the book is relatively free of errors.

PAUL M. HUMMEL
University of Alabama

Ordinary Difference-Differential Equations. By Edmund Pinney. University of California Press, 1958. 262 pp. $5.00.

In the last fifty years there has been a respectable number of mathematical articles treating integro- and difference-differential equations, but until the present volume appeared there has been no book in this field. The author's purpose is twofold: (i) to develop the general theory of a wide class of difference-differential equations and (ii) to give techniques for solving them. Integral transforms (with known inverses) play an important role in the theory which covers such types as first and second order mixed difference-differential equations with constant coefficients and one lag, and various mixed and nonmixed equations. Systems of mixed integro-differential and difference-differential equations with constant coefficients are also treated. A special feature of the book is the first practical treatment of a number of nonlinear equations, including Minorsky's equation. Applications are in many fields, including biology, economics, engineering and physics, and the book will be of great interest to all areas of applied mathematics in which the meaningful models involve a time lag. There are fourteen pages of bibliography.

CLETUS O. OAKLEY
Haverford College

BRIEF MENTION

101 *Puzzles in Thought and Logic.* By C. R. Wylie, Jr. Dover, New York, 1957. $1.00.

This collection of, for the most part, new logical puzzles will delight mathematicians everywhere. Certainly this low-cost volume belongs on the shelf of every mathematics library, both public and private. In fact, your reviewer feels it would be a welcome addition in a great many doctors' waiting rooms.

Calculus of Variations and Its Applications. Edited by Lawrence M. Graves. McGraw-Hill, New York, 1958. 153 pp. $7.50.

The papers of the Eighth symposium in Applied Mathematics, sponsored by the American Mathematical Society and the Office of Ordnance Research on April 12–13 at the University of Chicago, comprise the main meat of this up-to-date volume. The main topics include elasticity, plasticity, hydrodynamics, and dynamic programming.

The contributors include Eric Reissner, D. C. Drucker, Joseph B. Keller, J. B. Diaz, J. L. Synge, M. M. Schiffer, Richard Bellman, S. Chandrasekhar, and E. H. Rothe. In addition to the nine addresses, two brief notes by P. G. Hodge, Jr., and H. F. Weinberger are included. The individual papers either have been, or probably will be, reviewed in *Mathematical Reviews.*

Table for the Solution of Cubic Equations. By Herbert E. Salzer, Charles H. Richards and Isabelle Arsham. McGraw-Hill, New York, 1958. 161 pp. $7.50.

This tabular presentation will assist in obtaining rapid solutions of cubic equations using a desk calculator.

Analytic Geometry Problems. By C. O. Oakley. College Outline Series, Barnes and Noble, 1958. $1.95.

This excellent and extensive revision of Oakley's earlier work will be welcomed by mathematics students and teachers everywhere. The carefully-drawn figures, numerous illustrative examples, and excellent problems with answers, should make this small book a valuable adjunct for any textbook. Indeed, it could well be used as a text in itself.

Magic House of Numbers. Irving Adler. New American Library, New York, 1958. 123 pp. $.35.

This is an interesting collection of puzzles and tricks, available at your corner drugstore.

Education in Mathematics for the Slow Learner. By Mary Potter and Virgil Mallory. National Council of Teachers of Mathematics, Washington, D. C., 1958. 36 pp. $.75.

Mathematics Clubs in High Schools. By Walter H. Carnahan. National Council of Teachers of Mathematics, Washington, D. C., 1958. 32 pp. $.75.

This brief pamphlet contains the ideas of several teachers who have been connected with successful mathematics clubs. The wide spread interest in mathematics clubs may be judged by the phenomenal growth of the high school and junior high school mathematics club, Mu Alpha Theta, which is sponsored by the Mathematical Association of America. In one year's time this club has grown to more than two hundred eighty chapters in forty-six of the forty-nine states.

How to Use Your Library in Mathematics. By Allene Archer. National Council of Teachers of Mathematics, Washington, D. C., 1958. 6 pp. $.40

The Golden Number. By Borissavlievitch. Alec Tiranti, London. Philosophical Library, New York, 1958. 91 pp. $4.75.

More aesthetics than mathematics, but still interesting. Concerned primarily with the geometry of architecture.

History of Mathematics. Vols. I and II. By D. E. Smith. Dover, New York, 1958. Vol. I, 596 pp. $2.75, Vol. II, 725 pp. $2.75.

It is good to welcome back into print, in a relatively inexpensive edition, the well-known historical work of D. E. Smith.

Recreational Mathematics. By William L. Schaaf. National Council of Teachers of Mathematics, Washington, D. C., 1958. 151 pp. $1.20.

This valuable source book is a guide to the literature, prepared in a convenient form so that one may quickly learn where to look for information on the subject of interest. It certainly belongs in every mathematical library.

A Treatise on Plane and Advanced Trigonometry. By E. W. Hobson, Dover, New York, 1958. 383 pp. $1.95.

This reprint of Hobson's *A Treatise on Plane Trigonometry* should be required reading for all writers and teachers of elementary trigonometry.

Solid Geometry. By J. S. Hails and E. J. Hopkins. Oxford University Press, New York, 1957. viii+196 pp. $2.20.

This is a standard solid-geometry text for use in sixth-form courses in English schools. There is no hint of the combined analytic and synthetic approach which is currently being used in many of the more advanced American high schools.

The Taylor Series. By P. Dienes. Dover, New York, 1958. 552 pp. $2.75.

This reissue of Dienes' text, originally published by the Oxford Press, contains an investigation of analytic functions by means of Taylor Series, a useful adjunct for anyone studying complex variable.

Introduction to the Theory of Numbers. By Leonard E. Dickson. Dover, New York, 1958. 183 pp. $1.65.

A welcome republication of the original University of Chicago Press book. This reviewer had forgotten that Dickson's little book contains Siegel's proof on Thue's theorem on the rational approximations to a root of an algebraic equation.

Three Dimensional Dynamics. By C. E. Easthope. Academic Press, New York, 1958. viii+277 pp. $7.80.

This text, intended for undergraduate honor students, presents a vectorial treatment of solid dynamics without the use of tensors.

An Electronic Computer for Statistical Analysis of Radio Propagation Data. By M. Grønlund and C. O. Lund. Acta Polytechnica, Applied Mathematics and Computing Machinery Series, Vol. 1, No. 3, Copenhagen, 1957. $2.30 (address orders to Box 5073, Stockholm 5, Sweden).

The problems of statistical analysis of propagation data are considered and the equipment used is described in some detail in this Danish monograph.

An Introduction to the Theory of Random Signals and Noise. By Wilbur B. Davenport, Jr. and William L. Root. McGraw-Hill, New York, 1958. ix+393 pp. $10.00.

An introduction to the statistical theory needed to study signals and noises in communication systems by means of random processes. The Karhunen-Loeve expansion is used for random functions over a finite interval. This book provides another indication of the growing importance of advanced statistical procedures in engineering today.

Communication, Organization and Science. By Jerome Rothstein. Falcon's Wing Press, Indian Hills, Colorado, 1958. xcvi+110 pp. $3.50.

A discussion based upon the premise that measurement and communication have the same underlying logical structure. A number of the author's ideas are sufficiently provocative so that this reviewer recommends that anyone interested in information theory read it. The eighty-five page foreword by C. A. Muses is interesting in itself.

The Exterior Ballistics of Rockets. By Leverett Davis, Jr., James W. Follin, Jr. and Leon Blitzer. Van Nostrand, New York, 1958. v+457 pp. $8.50.

This well-motivated mathematical treatment of the exterior ballistics of rockets without moving control surfaces assumes a basic familiarity with analytical mechanics, differential equations, and vector analysis.

NEWS AND NOTICES

EDITED BY LLOYD J. MONTZINGO, JR., University of Buffalo

Readers are invited to contribute to the general interest of this department by sending news items to Lloyd J. Montzingo, Jr., Mathematical Association of America, University of Buffalo, Buffalo 14, New York. Items should be submitted at least two months before publication can take place.

PERSONAL ITEMS

University of Alaska: Dean William Cashen, Dean of Students and formerly head of department, will return as Professor; Dr. Torcom Chorbajian, Iowa State University, has accepted a position as Assistant Professor.

Brown University: Dr. W. H. Fleming, Purdue University, has been appointed Assistant Professor; Dr. Leon Greenberg, Yale University, has been appointed Instructor; Dr. A. M. Duguid has been appointed Research Associate in the Division of Applied Math.; Professor A. A. Bennett is now Professor Emeritus.

Millsaps College: Professor T. L. Reynolds is on sabbatical leave during the year 1958–59 at the U. S. Naval Ordnance Test Station in China Lake, California; Professor S. R. Knox is Acting Head of the Mathematics Department for the year 1958–59; Professor V. B. Temple, recently retired from Louisiana College, has been appointed Visiting Professor.

Mississippi Southern College: Associate Professor B. O. Van Hook has been promoted to Professor and made Chairman of the Department; Dr. G. W. Nicholson, University of Georgia, has been appointed Professor; Dr. R. W. Bagley, Lockheed, has been appointed Professor; Assistant Professor William Sanders, returning from three years study at the University of Illinois, has been appointed Associate Professor; Assistant Professor Virginia Felder, returning from a year's study at Columbia University, has been appointed Associate Professor; Mr. Gaston Smith, University of Alabama, has been appointed Assistant Professor.

West Virginia University: Mr. Bernard Gilbert, New York University, and Mr. H. W. Gould, University of North Carolina, have been appointed Instructors.

Assistant Professor W. S. Bicknell, University of Wisconsin, has been promoted to Associate Professor.

Assistant Professor C. H. Cunkle, Colorado State University, has been appointed Associate Professor at Dickinson College.

Assistant Professor D. E. Deal, Ball State Teachers College, will be studying at the University of Michigan on a Danforth Teacher Study Grant during 1958–59.

Dr. F. C. DeSua, Bell Telephone Laboratories, Whippany, New Jersey, has been appointed Associate Professor at the College of William and Mary.

Mr. L. T. Gardner, Oakwood School, Poughkeepsie, is now a graduate student at Columbia University and Part II Instructor for the Actuaries' Club of New York.

Dr. R. L. Graves, Standard Oil Co. of Indiana, Whiting, Indiana, has been appointed Assistant Professor of Applied Mathematics in the School of Business, and Associate Director of The Operations Analysis Laboratory at the University of Chicago.

Mr. J. G. Hankins, Jr., University of Oklahoma, has accepted a position as Geophysicist with the U. S. Navy Hydrographic Office, Washington, D. C.

Dr. D. K. Harrison, Brown University, has been appointed Assistant Professor at Haverford College.

Professor M. H. Heins, Brown University, has been appointed Professor at the University of Illinois.

Mr. Bruce Kellogg, Northwestern University, has accepted a position as Mathematician with Combustion Engineering, Windsor, Connecticut.

Dr. R. R. Kemp, Institute for Advanced Study, has been appointed Assistant Professor at Queen's University, Kingston, Ontario, Canada.

Dr. L. A. Kokoris, Washington University, will be a Visiting Associate Professor at the Illinois Institute of Technology during 1958–59.

Assistant Professor L. H. Lange, Valparaiso University, as the recipient of a Science Faculty Fellowship from the National Science Foundation, continues on leave at the University of Notre Dame.

Assistant Professor W. G. Lister, Brown University, has been appointed Professor at State University College on Long Island.

Professor Lee Lorch, Philander Smith College, is a Visiting Lecturer at Wesleyan University during 1958–59.

Mr. M. R. Luttrell, Western Electric Co., Chicago, Illinois, is now at Massachusetts Institute of Technology, Lincoln Laboratory, Lexington, Massachusetts, as a Defense Projects Engineer.

Assistant Professor R. T. J. Mahoney, United States Naval Academy, has been appointed Instructor at Washington University.

Mr. W. T. Neis, Aramco, Saudi Arabia, is now Mathematical Statistician, Bureau of the Census, Suitland, Maryland.

Assistant Professor F. R. Olson, University of Buffalo, has been promoted to Associate Professor.

Dr. G. A. Parkinson, University of Wisconsin-Milwaukee, is now Director, Milwaukee Vocational and Adult Schools.

Dr. R. F. Rinehart, Case Institute of Technology, is now in the Office of Ordnance Research, Duke University.

Dr. W. R. Seugling, Allstates Engineering Co., Trenton, New Jersey, is now Sr. Research Engineer, Rocketdyne Division of North American Aviation, Inc., Canoga Park, California.

Mr. L. C. Teng, Massachusetts Institute of Technology, is now a Research Associate, Engineering Research Institute of the University of Michigan.

Dr. R. L. Wilson, Convair, Ft. Worth, Texas, has been appointed Professor and Chairman of Department of Mathematics, Ohio Wesleyan University.

Assistant Professor J. E. Davis, University of Illinois, died March 1, 1958. He had been a member of the Association for 24 years.

Professor Emeritus E. H. Taylor, Eastern Illinois State College, died June 26, 1958. He was a charter member of the Association.

Mr. Jurio Tsuchiya, Mississippi State College, died June 28, 1958.

PRELIMINARY ACTUARIAL EXAMINATIONS PRIZE AWARDS

The winners of the prize awards offered by the Society of Actuaries to the nine undergraduates ranking highest on the score of Part 2 of the 1958 Preliminary Actuarial Examination are as follows:

First Prize of $200: Daniel G. Quillen, Harvard University

Additional Prizes of $100 each:

Edward J. Barbeau, Jr.	Toronto University
William H. Blake, Jr.	George Washington University
Theodore M. Jungreis	Rensselaer Polytechnic Institute
David H. Krantz	Yale University
Joe Lipman	Toronto University
Dennis W. Moore	Harvard University
Theodore S. Rosky	State University of Iowa
Lawrence A. Shepp	Brooklyn Polytechnic Institute

The Society of Actuaries has authorized a similar set of nine prizes for the 1959 examinations on Part 2.

The 1959 Preliminary Actuarial Examinations will be prepared by the Educational Testing Service under the direction of a committee of actuaries and mathematicians and will be administered by the Society of Actuaries at centers throughout the United States and Canada on May 13, 1959. The closing date for applications is April 1, 1959.

THE MATHEMATICAL ASSOCIATION OF AMERICA

Official Reports and Communications

NEW MEMBERS

Professor H. M. Gehman, Secretary-Treasurer, announces that the following 154 persons have been elected to membership by the Board of Governors on applications duly certified.

ESTHER ADLER, M.A. (Columbia) Lecturer, Yeshiva University

GARY L. ANDERSON, Student, Bemidji State College.

DAVID R. ANDREW, Student, Southwestern Louisiana Institute.

PAUL ARMER, A.B. (U.C.L.A.) Head, Numerical Analysis, RAND Corp., Santa Monica, California.

CHARLES H. ARNOLD, M.A. (Lehigh) Teacher, Chestnuthill High School, Brodheadsville, Pennsylvania.

JAMES L. BAILEY, Ph.D. (Michigan S.U.) Asst. Professor, Case Institute of Technology.

MRS. SARABETH T. BARNES, M.S. (Wisconsin) Instr., University of Minnesota.

LT. DAVID R. BARR, M.S. (Miami, Ohio) United States Air Force, Iowa City, Iowa.

BENJAMIN BAUMSLAG, Student, University of Witwatersrand, South Africa.

NORMAN F. BEACH, A.B. (Princeton) Asst. Supt., Film Emulsion Division, Eastman Kodak Co.

RICHARD W. BEALS, Student, Yale University.

MORTON P. BERENSON, Student, University of Oregon.

DAVY L. BERNARD, Student, Southwestern Louisiana Institute.

RAYMOND C. BOEHNE, Student, University of Detroit.

KAYLAND Z. BRADFORD, Student, University of Oklahoma.

PEDRO BRICENO, Licenciatura (Central U. of Venezuela) Actuary, Ministry of Labor, Caracas, Venezuela.

WILLIAM T. BROOKS, B.S. (Texas Tech) Industrial Engineer, Astrodyne, McGregor, Texas.

DORETTA M. BROWN, Student, Ursinus College

CAPT. EDWIN E. BROWN, B.S. (Florida S.U.) U.S.A.F.; Grad. Student, Stanford University.

JAMES W. BROWN, M.A. (Michigan) Teaching Fellow, University of Michigan.

JOHN A. BROWN, Ph.D. (Wisconsin) Professor, Oneonta State Teachers College, New York.

JAMES P. BURLING, M.A. (N.Y.S.C. for Teachers) Asst. Professor, Oneonta State Teachers College, New York.

LINDA M. BUSWELL, Student, Carleton College.

WILLIAM F. CARPENTER, B.S.E.E. (Florida) Grad. Asst., University of Florida.

JOHN G. COOK, Student, University of British Columbia.

HUGH R. COOMES, Student, University of Kentucky.

WALTER E. CRAIG, Student, St. Martin's College.

HOBART L. CURTIS, Student, San Jose State College.

JOHN O. DANIELSON, M.S. (Wisconsin) Dean of Instruction and Chairman of Dept., Wisconsin State College.

REV. BRENDAN P. DONNELLY, OSB, B.A. (St. Anselm's) Instr., St. Anselm's College.

NETTIE A. DOOLITTLE, Ed.D. (Missouri) Asst. Professor, University of Missouri.

CHARLES DRESCHER, B.S. (Poly. Inst. of Brooklyn) Asso. Equipment Engineer, Western Electric Co., New York City.

FORREST E. DRISTY, B.S. (S. Dakota Sch. of Mines & Tech.) Instr., South Dakota School of Mines and Technology.

DANIEL E. DUPREE, B.S. (Louisiana Poly. Inst.) Grad. Student, Alabama Polytechnic Institute.

ALEXANDER DURLEY, M.A. (Atlanta) Instr., Texas State University.

FRANCES P. DUSHEK, M.A. (Texas) Instr., Del Mar College.

BRUCE ERICKSON, Student, University of British Columbia.

MARIO V. FIONDELLA, M.S. (Florida) Instr., University of Florida.

MARY L. FISHER, M.S. (Illinois) Chairman of Dept., Joliet Township High School and Junior College, Illinois.

JAMES L. FLATT, M.A. (Peabody) Asst. Professor, Clemson College.

NEAL E. FOLAND, M.A. (Missouri) Instr., University of Missouri.

ROBERT M. FOSSUM, Student, St. Olaf College.

JAMES K. FOSTER, Student, University of Minnesota.

KENNETH A. FOWLER, Ph.D. (Michigan) Asst. Professor, San Jose State College.

JOSEPH A. FROMME, Student, Purdue University.

LOUIE R. GIESZL, Student, University of Houston.

JIMMIE D. GILBERT, M.S. (Alabama Poly. Inst.) Instr., Alabama Polytechnic Institute.

MYRNA C. GILES, Student, University of Omaha.

MAURICE E. GILMORE, JR., Student, Georgetown University.

RONALD L. GRAHAM, Student, University of Alaska.

WILLIAM M. GRAVES, Student, Georgia Institute of Technology.

LAWRENCE F. GUSEMAN, JR., Student, A. & M. College of Texas.

JOSEPH M. C. HAMILTON, M.A. (U.C.L.A.) Instr., Los Angeles City College.

PAUL M. HARMS, A.B. (Bethel) Grad. Asst., Iowa State College.

DOUGLAS C. HARVIE, M.S. (Victoria) Lecturer, Victoria University of Wellington, N. Z.

ROBERT J. HENDERSON, Student, University of British Columbia.

JOHN R. F. HEWETT, Student, University of Toronto.

WILLIAM B. HIGGINS, M.A. (Columbia T.C.) Asst. Professor, Ball State Teachers College.

PAUL D. HILL, M.S. (Alabama Poly. Inst.) Grad. Student, Alabama Polytechnic Institute.

C. ROBERT HILLAND, Student, A. & M. College of Texas.

JOHN W. HOGAN, A.B. (Berea) Teaching Asst., University of Wisconsin.

LEONARD I. HOLDER, Ph.D. (Purdue) Asst. Professor, San Jose State College.

JOHN E. HOMER, JR., Student, State University of Iowa.

EDGAR H. HOPPER, M.S. (Tennessee) Instr., Alabama Polytechnic Institute.

RICHARD L. HOTCHKISS, Student, University of Minnesota.

WILLIAM A. HUSTED, Student, Hobart College.

ROBERT J. IRWIN, B.S. (Case Inst.) President, Eddie Painton Associates, Cleveland, Ohio.

RICHARD L. JACOBSEN, Student, St. Olaf College.

WILBUR J. JONSSON, B.S. (Manitoba) Summer Student, Defence Research Board, St. Hubert, Quebec.

LEWIS S. KARSH, Student, Wesleyan University.

RICHARD E. KEEFFE, B.S. (Buffalo) Engineer, Rocketdyne, Canoga Park, California.

DENIS J. KIELY, JR., B.E.E. (Santa Clara) Instr., San Jose State College.

JAMES I. KILLIAN, Student, University of Oklahoma.

RICHARD L. KINKEAD, Student, University of Houston.

CLAUDE A. KIRKPATRICK, Student, University of Oklahoma.

ROBERT E. KIRSAMMER, Student, University of Detroit.

MRS. DOROTHY J. KNIGHT, M.A. (Kent S.U.) Asst. Professor, Muskingum College.

DAVID H. KRANTZ, Student, Universite de Nancy, France.

SAMUEL S. KUTLER, B.A. (St. John's, Annapolis) Asso. Math., Johns Hopkins University.

FRANK W. LANE, M.A., M.S. (St. Bonaventure) Asso. Professor, Ohio Northern University.

FREDERICK L. LAWSON, Student, Southwestern Louisiana Institute.

JOSEPH Lev, Ph.D. (Cornell) Acting Chief, Bureau of Statistical Services, New York State Educational Dept., Albany, New York.

LAWRENCE A. LIDDIARD, Student, University of Minnesota.

JERRY L. LINNSTAEDTER, Student, A. & M. College of Texas.

JAMES N. MARTIN, Student, Texas Christian University.

HARRY T. MATHEWS, Student, Georgia Institute of Technology.

JOSEPH L. MAZANEC, M.S. (Wisconsin) Instr., Los Angeles City College.

ESTELLE MAZZIOTTA, M.A. (U.C.L.A.) Instr., Los Angeles City College.

VAN K. MCCOMBS, B.S. (Mississippi S.C.) Grad. Student, Mississippi State College.

THOMAS S. MCFEE, B.S. (Maryland) Math., David Taylor Model Basin.

JACK L. MCGEE, B.S. (Oklahoma) Jr. Engineer, Temco Aircraft Co., Garland, Texas.

GEORGE J. MICHAELIDES, M.S. (Virginia Poly. Inst.) Instr., Lamar State College of Technology.

CAPT. WALTER R. MILLIKEN, B.S. (U.S. Military Academy) Asst. Professor, U.S.A.F. Academy.

CHESTER L. MIRACLE, M.S. (Alabama Poly. Inst.) Grad. Student, University of Kentucky.

BRUCE J. MOODY, Student, University of Oklahoma.

MRS. DORIS L. MOORE, M.A. (Western Carolina) Grad. Student, University of Virginia.

WILLIAM R. NEAL, Student, Arizona State College.

KEITH H. NICAISE, Student, Mississippi State College.

TERRY P. NORRIS, Student, Arizona State College.

KARL K. NORTON, Student, Yale University

WORTH D. NOWLIN, JR., Student, A. & M. College of Texas.

ROBERT D. OBERG, B.S. (Minnesota, Duluth) Grad. Student, University of Minnesota.

LLOYD D. OLSON, M.Ed. (N. Dakota Agric. Coll.) Instr., North Dakota Agricultural College.

HARLAN S. PAFFORD, M.Ed. (Virginia) Teacher, Marion High School, Virginia.

CHARLES E. PETTYPOOL, JR., M.A. (Ohio S.U.) Instr., Eastern Illinois University.

GEORGE W. PETZNICK, JR., Student, Case Institute of Technology.

ROGER A. PURVES, B.A. (British Columbia) Grad. Student, University of British Columbia.

ARLAN B. RAMSAY, Student, University of Kansas.

JOHN R. REAY, B.A. (Pacific Lutheran) Acting Instr., University of Idaho.

CHAVIS L. RENWICK, JR., M.S. (N. Carolina Coll.) Statesville, North Carolina.

WAYNE H. RICHTER, Student, Swarthmore College.

MRS. AGNES Y. RICKEY, M.S. (Barry) Supervisor, Dade County Board of Public Instruction, Miami, Florida.

GEORGE A. RIETZ, B.S.E.E. (S. Dakota S.C.) Ed. Program Development, General Electric Co., New York City.

REINO R. RIIHONEN, Bon Marche, Spokane, Washington.

SHELDON T. RIO, M.A. (Montana S.U.) Grad. Student, Oregon State College.

THACHER T. ROBINSON, M.A. (Princeton) Chappaqua, New York.

JIMMIE H. ROGERS, B.A. (Oklahoma Baptist) Instr., Connors State Agricultural College.

JOSEPH S. ROMANOW, Student, Tufts University.

JORDAN T. ROSENBAUM, Student, Case Institute of Technology.

GEORGE N. ROUNTHWAITE, Student, San Diego State College.

MRS. ISABELLE P. RUCKER, B.A. (Randolph-Macon) Teacher, Louisa County School Board, Virginia.

DAVID H. SANDERS, Student, Princeton University.

RICHARD F. SHEPARD, A.M. (Columbia) Math. Editor, Henry Holt & Co., New York City.

TADAO SHINGU, B.S. (Kyoto, Japan) Asst. Professor, Shimane Agricultural College, Japan.

PETER SIKORYAK, Student, Hobart College.

FRANCIS E. SIWIEC, Student, Carteret School, W. Orange, New Jersey.

RALSTON J. SMITH, Student, Eastern Kentucky State College.

SAMUEL SOBEL, B.S. (C.C.N.Y.) Reliability Engineer, Sperry Gyroscope Co., New York.

HAROLD S. SPRAKER, M.Ed. (Virginia) Grad. Student, University of Virginia.

HENRY E. STERN, B.E. (Tulane) Asso. Scientist, Lockheed Aircraft Corp., Marietta, Georgia.

JOHN E. STROUT, B.S. (Illinois) Grad. Asst., University of Illinois.

ROBERT L. STURGEON, Student, University of British Columbia.

DONALD H. TARANTO, B.S. (C.C.N.Y.) Applied Science Rep., I.B.M., New York.

MRS. DINA G. S. THOMAS, M.A. (Utah) Instr., University of Colorado.

JOHN A. THORPE, Student, Massachusetts Institute of Technology.

CARL L. TIBERY, B.S. (Bates) Asst. Instr., University of Maryland.

GEORGE G. TOWN, M.S. (Wisconsin) Boeing Research Asso., Oregon State College.

BENJAMIN A. TRIMBLE, Decatur, Georgia.

HWA TSANG, Student, University of Chicago.

OSCAR VALDIVIA G., B.S. (San Marcos, Peru) Asso. Professor, Universidad de Trujillo, Peru.

WILLIAM A. VEECH, Student, Dartmouth College.

GUY E. WEBBER, JR., B.S. (Emory & Henry) Teacher, Edgewood, Maryland.

RUSSELL A. WELKER, M.S. (Illinois) Grad. Asst., University of Illinois.

ALAN J. WESTCOTT, Student, University of California.

BRANDON W. WHEELER, Student, Sacramento State College.

ALTON L. WILKINSON, Student, A. & M. College of Texas.

JAMES P. WILLIAMS, Student, University of Detroit.

FLOYD D. WILDER, Student, Central State College.

ALAN WILSON, Ph.D. (Rice Institute) Houston, Texas.

GERALD WOHL, B.A. (Syracuse) Field Engineer, General Electric Co., San Francisco, California.

JOHN E. WOOD, M.A. (Longwood) Instr., Hampden Sydney College.

ROY E. WORTH, Student, University of Georgia.

JOHN W. WYMAN, Student, Olivet Nazarene College.

EDWARD G. ZDINAK, M.S. (Pittsburgh) Grad. Student, University of Pittsburgh.

THE MAY MEETING OF THE INDIANA SECTION

The thirty-fifth annual meeting of the Indiana Section of The Mathematical Association of America was held at Ball State Teachers College, Muncie, Indiana, on Saturday, May 3, 1958. Professor C. B. Gass of DePauw University, Chairman of the Section, presided at both morning and afternoon sessions. There were 52 in attendance, including 39 members of the Association.

The following officers were elected: Chairman, Professor G. N. Wollan of Purdue University; Vice-Chairman, Professor K. H. Carlson of Valparaiso University; Secretary-Treasurer, Professor C. F. Brumfiel of Ball State Teachers College.

Professor Edwards, chairman of the Committee on Awards, announced that four Association Medals had been awarded this year to high school seniors exhibiting high mathematical achievement in the Indiana Science Talent Search program. The following motions were carried: (1) That the Section adopt the policy of holding a fall meeting in joint session with the Mathematics Division of the Indiana Academy of Science. (2) That the Section sponsor the administration in Indiana of the Annual High School Mathematics Contest which is sponsored nationally by the M.A.A. and the Society of Actuaries. (3) That a committee be appointed by the chairman to work with the Indiana Council of Teachers of Mathematics to lay down a plan for securing support for local institutes on the teaching of mathematics.

Professor R. M. Thrall of the University of Michigan gave the invited hour address on the topic, "Applications of Mathematics in the Social Sciences."

The following short papers were presented:

1. *Some remarks on the teaching of elementary algebra*, by Professor A. M. Yaqub, Purdue University.

In attempting to strengthen our undergraduate mathematics courses, the author proposed to combine *understanding* with techniques in the teaching of elementary algebra. In algebra, as in high school geometry, one would naturally begin with the axioms which the real numbers are supposed to satisfy, and from which the theorems are to be derived. These axioms include the usual axioms for a field. On the basis of these one could derive the familiar laws of signs. By assuming a few additional axioms one could then derive the laws of inequalities and the laws of exponents. This modest start would immediately indicate to the student the spirit of the axiomatic approach, and no doubt show him that algebra is every bit as suitable for axiomatic treatment as geometry. Moreover, this method allows the teaching of algebra as a *science* rather than as a collection of recipes together with some mystical laws.

2. *Dexinal gauges*, by Mr. Aaron Miller, 1415 W. 28th Street, Indianapolis, Indiana.

The stop to which the base 2 must be raised to produce a number k is called the dexinal gauge of k. Two numbers are dexinated by adding their gauges and are sindexinated by subtracting their gauges. A dexratio (dexine of a ratio) is the dexnum (dexine of the numerator) sindexed by the dexdenom (dexine of the denominator). A dexratio is reduced by taking the ratio of the logarithms to the base 2 of the dexnum and dexdenom. The equality of the two dexratios is called a poise and is the analogue of a proportion. The mean poisal is the analogue of the mean proportional. Employing these definitions, the author developed some theorems and presented several interesting applications in numerical computations.

3. *The seventeen ornamental groups*, by Professor H. W. Alexander, Earlham College.

The seventeen ornamental groups were discussed from the standpoint of (a) the classification of an actual design under one of these groups and (b) the representation of the groups by means of matrices. Other designs were examined.

4. *The sum of a particular series and the corresponding integral*, by Professor L. W. Stark, Butler University.

The analytic solution of the heat conduction equation is obtained by use of the Laplace transform and the convolution integral. One term in the solution is the cosine series

$$\sum_{n=1}^{\infty} [(-1)^{n-1} \cos (2n-1)y/(2n-1)^{2p-1}]$$

$p \geq 1$. Beginning with the result given by Bromwich for $p=1$, the method for obtaining the result for $p=2$ was given in detail and results were then stated for $p=3, 4, 5$. It was also established that the summations evaluated at $y=0$ are multiples of corresponding Euler numbers.

5. *A progress report on experimental work at Ball State Teachers College*, by Professor C. F. Brumfiel, Ball State Teachers College.

For the last three years an experimental geometry and algebra program has been tested in the Ball State laboratory school. Tenth grade geometry is treated rigorously in a course based upon a modified version of the Hilbert postulates. The algebra is a mild postulational treatment that covers most of the conventional topics of ninth grade algebra. During the past year teachers from Eastern Indiana schools, enrolled at Ball State in a National Science Foundation In-Service Institute, have taught the geometry experimentally. Under a continuation of this grant the experimental program will be continued and expanded to include the algebra in 1958–59.

6. *It's all in your mind*, by Professors J. E. Forbes and W. R. Fuller of Purdue University, presented by Professor Forbes.

This was a preliminary report on an experiment in commercial television in a series of weekly broadcasts of topics in mathematics. Many interesting points concerning the preparation and presentation of the programs and the methods used to enlist and maintain the interest of listeners were discussed.

7. *A report on the 1957 Summer Institute on Mathematics in the Social Sciences at Stanford University*, by Professors J. C. Polley, Wabash College, G. N. Wollan, Purdue University, and K. H. Carlson, Valparaiso University.

The subject was introduced by Mr. Polley with general remarks on the nature, the staff, and the organization of the institute. He stated that the institute had been sponsored by and financed by a grant from the Social Science Research Council for the purpose of acquainting college teachers of mathematics with the current applications of mathematics in the field of the social sciences. Attending members represented colleges of various types widely distributed over the country.

Drawing on the eight-weeks experience, Mr. Wollan emphasized the values of such institutes. He urged that efforts be made to promote setting some up on the local level.

In conclusion, Mr. Carlson discussed in some detail the conduct of the institute and the material presented by the various members of the staff.

J. C. POLLEY, *Secretary*

THE MAY MEETING OF THE MINNESOTA SECTION

The annual spring meeting of the Minnesota Section of the Mathematical Association of America was held on May 17, 1958 at St. John's University, Collegeville, Minnesota. Reverend Walbert Kalinowski, O.S.B., of St. John's University presided at the morning session. The section chairman, Professor O. E. Stanaitis of St. Olaf College, presided at the afternoon session. There were 53 persons registered, of whom 39 were members of the Association.

The following officers were elected to serve for the academic year 1958–1959: Chairman, Reverend Walbert Kalinowski, O.S.B., of St. John's University; Secretary, Professor F. L. Wolf of Carleton College; Members of the Executive Committee, Professor O. E. Stanaitis of St. Olaf College, Professor David Lewis of Hamline University and Remington-Rand Univac, and Professor James Serrin of the University of Minnesota.

At the business meeting, Professor J. M. H. Olmsted reported on the High School Mathematics Contest which was sponsored by the section in Minnesota this year. In this, the first year that the contest was given in Minnesota, it was very successful. The section owes many thanks to Professor G. K. Kalisch of the University of Minnesota and to the members of his High School Contest Committee for this success. Professor Leon Green of the University of Minnesota was appointed chairman of the High School Contest Committee for 1958–1959.

Professor F. L. Wolf reported for the Committee on High School-College Relations. Several proposals for the improvement of high school-college relations were made by the committee and motions from the floor were passed instructing the committee to proceed with implementation or further study of these.

The following papers were presented:

1. *Equations with trigonometric values as roots*, by Professor K. W. Wegner, Carleton College.

Sixty-four equations were presented, along with illustrations of their use in the classroom, as the only irreducible polynomial equations with integral coefficients and of degree two through seven whose roots are of the form $\pm\sin y$, $\pm\cos y$, $\pm\tan y$, $\pm\cot y$, $\pm\sec y$, or $\pm\csc y$, where y is a rational number of degrees.

2. *Five mutually-tangent spheres*, by Mr. H. E. Fiala, North Dakota State College, introduced by Professor Ruby M. Grimes.

This paper explains the problem of Five Mutually Externally Tangent Spheres. It gives also the general solutions for the volume of an irregular tetrahedron and the radii of its inscribed and its circumscribed spheres. It then shows how the concept of five tangent spheres can be applied to greatly simplify the solutions to most problems dealing with properties of tetrahedrons. The principle involved is essentially a change of variables to reduce the number of unknowns. It suggests also how the concept of five tangent spheres can be applied in designing an inertial guidance system.

3. *Mathematical machines and mathematicians*, by Professor S. C. Kleene, University of Wisconsin.

The class of all functions which can be computed, and of all relations (predicates) which can be decided by machines, is characterized. On the basis of this characterization examples are given of functions which cannot be computed, and of relations which cannot be decided, by machines. (This paper is an exposition of results originally obtained independently, in different forms, by Alonzo Church and by A. M. Turing in 1936. See the speaker's *Introduction to Metamathematics*, New York, 1952, or his lecture notes *Sets, Logic and Mathematical Foundations*, Williams College, 1956, or Martin Davis *Computability and Unsolvability*, New York, 1958).

4. *The oscillation in sign of solutions of linear, ordinary difference equations with constant coefficients*, by Professor Murray Braden, Macalester College.

In investigating the oscillation in sign of solutions of the infinite strip problem for a general class of partial difference operators, Fulton Koehler and the author found it desirable to prove the theorem: "Every nontrivial, real solution of an ordinary, linear, homogeneous difference equation with real, constant coefficients must oscillate in sign infinitely often as x approaches infinity." In the course of the proof, two lemmas were established concerning trigonometric sums of the form $S(x)=\sum_{j=1}^{n}(c_je^{i\theta_jx}+c_je^{-i\theta_jx})$, where $x=0, 1, 2, \cdots$. These are: (1) $S(x)$ will approximate itself as closely as desired for an infinite number of values of x; (2) $S(x)$ must be positive for at least one value of x, and negative for at least one value of x.

5. *Boolgebra: ands, ors, and nots, among other things*, by Dr. D. M. Brown, Remington Rand UNIVAC.

Boolean Algebra may be considered as a means of "mixing" binary information (signals, statements, *etc.*) by using combinations of three mixing devices called AND, NOT, and OR. The NOT device has one input and one output, while each of the AND and OR devices has two inputs and one output.

There are exactly four devices with one input and one output, and exactly sixteen devices with two inputs and one output. Mechanical equipment implementing each device, using two sizes of balls as the binary inputs and outputs is demonstrated. The Boolean equation for each device is presented, along with a schematic diagram and an output ("truth") table.

F. L. WOLF, *Secretary*

THE MAY MEETING OF THE UPPER NEW YORK STATE SECTION

The fourteenth annual meeting of the Upper New York State Section of the Mathematical Association of America was held at the University of Montreal, Montreal, Quebec, Canada, on May 10, 1958. The Chairman of the Section, Professor E. E. Haskins of Clarkson College of Technology, presided at the morning session, and the Vice-Chairman, Professor Caroline A. Lester of the New York State College for Teachers at Albany, presided at the afternoon session. There were 91 persons in attendance, including 54 members of the Association.

At the business meeting the following officers were elected: Chairman, Professor Caroline A. Lester, New York State College for Teachers at Albany; Vice-Chairman,

Professor Dis Maly, Rensselaer Polytechnic Institute; Secretary-Treasurer, Professor N. G. Gunderson, University of Rochester. A report from a committee of department chairmen was heard to the effect that the New York State Education Department had been contacted and made aware of the opposition of the Section to the specific requirements added for accreditation in teaching mathematics in New York State and to the added requirements in education.

A Committee on the Strengthening of Mathematics in the Section reported on its activities and studies. One recommendation was that individual colleges and departments of mathematics make known their views on the teacher certification problem. Another was that schools give more attention to the Advanced Placement Program. The Committee warned of the danger in attracting more students in Mathematics without strengthening teaching. It was voted that this Committee be continued for another year.

Professor A. J. Coleman of the University of Toronto reported on the extension of the Mathematics Contest into Canada. This year over 1000 students from 41 schools participated. Professor Nura Turner of the New York State College for Teachers reported on the Contest in New York State (exclusive of the metropolitan area and the western counties). This year, the first for this area, 3729 students from 211 schools participated.

The program was as follows:

1. *The Canadian Mathematical Congress*, by Professor R. L. Jeffery, Queen's University. (By invitation.)

The speaker, who is President of the C. M. C., gave a history of the Congress, and described the organization, activities, and plans of the group.

2. *Training teachers of mathematics*, by Professor A. Wittenberg, Laval University. (By invitation.)

The crucial issue in the teaching of mathematics is the adequate training of the teachers. A thorough mathematical training is necessary, but not enough. A teacher must be emotionally committed to teaching, able to see elementary mathematics in their own right, able to teach them without taking for granted the mathematical way of thinking. The speaker suggests a teacher training program including: 1) a thorough introduction to mathematics and their main applications; 2) a good introduction to those subjects enabling a teacher to see mathematics in context—foundations, philosophy, and history of mathematics; 3) on the basis of such knowledge, a thorough and independent examination of elementary mathematics.

3. *A mathematical analysis of the English verb-phrase*, by Professor Joachim Lambek, McGill University.

The method of syntactic types, due to Ajdukiewicz, Bar-Hillel and the author, is used to analyse the English verb-phrase. After suitable types have been assigned to all the forms of the verbs *must*, *work*, *like*, *have*, *be*, *etc*, it becomes possible to decide by a mathematical computation whether any given arrangement of these forms, together with the names *John*, *Jane*, *etc.*, constitutes a grammatical sentence, such as *John must have been liking Jane.*

4. *The logic of algebras and the algebra of logic*, by Professor L. O. Kattsoff, Harpur College.

There is need to distinguish between an algebra which can be interpreted in terms of propositions, conjunction, negation and implication, and the modes of reasoning used in demonstration. In a sense, it is misleading to speak of the algebra of logic. What we have is simply an abstract algebra. When this abstract algebra is interpreted as a logic, there is already implied an intuitive logic, presupposed by the interpretation. If not, an infinite regression of rules of logic develop. A similar distinction is needed between finite induction as a property of a well-ordered system, and as a mode of demonstration.

5. *Convex representations of planar graphs*, by Professor W. T. Tutte, University of Toronto.

Let G be a triply connected graph, known to be planar. We consider the problem of constructing a representation of G in the plane such that the edges are represented by straight lines and each residual domain is the interior or exterior of a convex polygon. It is found that the vertices of such a representation can be obtained by solving certain linear equations, with arbitrary positive coefficients, associated with the graph. In the simplest representation of this kind the vertices of one circuit of G are represented by the vertices of a convex polygon, arbitrary except for the number of its vertices, and every other vertex is at the centroid of the vertices to which it is directly joined.

6. *The spherical image*, by Professor C. S. Ogilvy, Hamilton College.

If all the unit normal vectors of a regular region of a surface are moved to the origin, their end points describe the spherical image of the region on the unit sphere. This mapping by parallel normals is well known to be conformal if and only if the region is part of a minimal surface or of a sphere. It can be shown that the mapping of the general (non-minimal) surface of negative Gaussian curvature can be described locally by decomposing it into three linear transformations: a rotation through 90°, a reflection, and a certain (specified) simple shear.

7. *On the classical characterizations of the existence a.e. of a derivative for functions of one real variable*, by Professor A. G. Fadell, University of Buffalo.

The best-known condition for the existence a.e. of a derivative for functions of one variable is bounded variation. This condition, of course, is not necessary. The classical characterization apparently is not well known, as evidenced by its absence from the recent wealth of real-variable texts. In this note we outline the proof of the classical necessary and sufficient condition for measurable functions, namely the existence a.e. of locally bounded difference quotients. The proof utilizes the sufficiency of a Lipschitz condition on an open set, the Lipschitz extension theorem, elementary decomposition theorems, and aspects of Lebesgue density.

8. *The minimax theorem (another simple proof)*, by Professor J. E. L. Peck, McGill University.

Another simple proof of the minimax theorem is given, which applies equally well to the case where only one space of pure strategies is finite. The method uses properties of linear functions on convex sets.

N. G. GUNDERSON, *Secretary*

THE JUNE MEETING OF THE PACIFIC NORTHWEST SECTION

The eleventh annual meeting of the Pacific Northwest Section of the Mathematical Association of America was held at Oregon State College, Corvallis, Oregon on June 20, 1958 in conjunction with the 547th meeting of the American Mathematical Society and an organizational meeting of the Pacific Northwest Section of the Society for Industrial and Applied Mathematics. Professor Sydney Hacker, Chairman of the Section, presided over the meetings. There were 133 persons in attendance, including 82 members of the Association.

The following officers were elected: Chairman, Professor Kenneth Bush, University of Idaho; Vice-Chairman, Professor Arthur Livingston, University of Washington; Secretary-Treasurer, Professor K. S. Ghent, University of Oregon. Brief reports were given concerning the High School Mathematics Contest for British Columbia, Idaho and Oregon. The contest was not sponsored in Montana by the Section.

The program included a session for contributed papers, an invited address by Professor Arthur Erdelyi, three invited half-hour talks, and four fifteen-minute talks on problems of high school mathematics teaching. Professor Lonseth introduced Professor

Erdelyi; Professor Keeping introduced the three lecturers for the half-hour talks and Professor Vatnsdal presided at the evening session. The abstracts for the papers are given below.

Contributed papers (10 minutes):

1. *Classical orthogonal polynomial transforms*, by Dr. T. P. Higgins, Dalmo Victor Company, Belmont, California.

Integral transforms are often useful in solving boundary-value problems when the nature of the transform is such that it can be applied to replace a particular group of terms of the differential equation with a single simple term. Various authors have considered the particular advantages of this type of integral transform. A generalization of the Jacobi transform can be made using a more general polynomial kernel, and this transform reduces, under special choices for certain of the parameters, to either the Jacobi transform, the Gegenbauer transform, the Legendre transform, the Tchebichef transform, the Laguerre transform, or the Hermite transform. This note defines the classical orthogonal polynomial transform, proves its characteristic property, and gives simple examples of applications of the characteristic property.

2. *A method for solving the quartic equation*, by Dr. C. E. Sealander, Mathematical Research Laboratory, Boeing Scientific Research Laboratories, Seattle, Washington.

Consider the quartic equation $f(x)=x^4+bx^3+cx^2+dx+e=0$. The substitution $x=my+n$ transforms this equation to $(my)^4+(1/6)f'''(n)(my)^3+(1/2)f''(n)(my)^2+f'(n)my+f(n)=0$. This is a reciprocal equation if (1) $f(n)=m^4$ and (2) $m^3f'''(n)=6mf'(n)$. The latter two equations can be solved simultaneously for m and n, and the substitution $y+1/y=z$ for solving reciprocal equations then yields the solution of the quartic. Elimination of m from equations (1) and (2) yields a resolvent cubic of the form (3) $An^3+Bn^2+Cn+D=0$. Three exceptional cases are discussed: (I) The case $A=B=C=D=0$; (II) $n=-b/4$ is a root of equation (3); and (III) $f'(n)=0$, $f'''(n)\neq 0$.

3. *Incomplete elliptic integrals of the third kind*, by Dr. R. G. Selfridge and Dr. J. E. Maxfield, U. S. Naval Ordnance Test Station, China Lake, California, presented by Dr. Selfridge.

The incomplete elliptic integral of the third kind is given by $\pi(\phi, \alpha^2, k)=\int_0^{\phi}(1-\alpha\sin^2\theta)^{-1}\cdot(1-k^2\sin^2\theta)^{-1/2}d\theta$, and occurs in many aerodynamic and hydrodynamic problems. One of the difficulties associated with tabulating this function is that of checking the results. A simple and effective check is available if an independent computation can yield the complete integral ($\phi=\pi/2$). Previous methods of computation of the complete integral proved difficult to handle in that convergence of the numerical methods proved exceedingly cumbersome. The final method chosen was that of solving the differential equation (with respect to k), that is satisfied by the complete integral. This involved some careful handling because of the singularities of the equation but provided a very effective check on the computations. The resultant table is in press at Dover Publications.

Invited address:

Operational calculus and generalized functions, by Professor Arthur Erdelyi, California Institute of Technology.

Expository account of J. Mikusinski's work (Rachunek operatorow, 1953) which provides a mathematical background both for Heaviside's operational calculus and for delta functions and other "improper functions." This calculus has been applied successfully to ordinary differential equations, integral equations, and hyperbolic and parabolic partial differential equations.

Invited thirty-minute talks:

1. *The problem of optimal control*, by Professor D. W. Bushaw, Washington State College.

The problem arises out of that of designing a control system in which the available control force is bounded and the object is to reduce the difference between the current and desired outputs,

together with all time derivatives of this quantity, to zero as rapidly as possible. It has been conjectured (in the so-called "Bang-Bang Principle") that in any solution of this problem only the extreme values of the control force will be used. The current mathematical status of this principle was discussed, and various solved and unsolved questions connected with it were described.

2. *Variational principles and eigenvalues*, by Professor H. J. Sagan, University of Idaho.

Let L be a self-adjoint linear differential operator and consider the homogeneous boundary value problem $L(u)+\lambda ru=0$ with $u+\alpha(\partial u/\partial n)=0$ on the boundary. In general there are infinitely many values λ_k of λ (Eigenvalues) for which this problem has nontrivial solutions (Eigenfunctions). These Eigenfunctions u_k turn out to be solutions of a variational problem of the type $I(u)/C(u)\rightarrow$minimum where I and C are positive definite quadratic functionals and where u has to be orthogonal, with the weight function r, to the preceding $k-1$ Eigenfunctions. The corresponding Eigenvalues λ_k are given by the minima of I/C. This principle—widely referred to as "Rayleigh's Principle"—opens up possibilities for numerical computations of upper and lower bounds of the Eigenvalues as suggested by Ritz and Weinstein.

3. *Approximation by polynomials with integral coefficients*, by Professor Edwin Hewitt and Professor H. S. Zuckerman, University of Washington, presented by Professor Hewitt.

Let X be a compact Hausdorff space, $\mathfrak{C}(X)$ the set of all real-valued continuous functions on X, and $\mathfrak{F}$ a subset of $\mathfrak{C}(X)$ separating points of X. Let $\mathfrak{P}$ be the set of all functions on X that are polynomials with integral coefficients in functions from $\mathfrak{F}$. Let $\mathfrak{B}=\{g: g\in\mathfrak{P},\ 0\leq g(x)<1\}$ for all $x\in X$. Let $J=\cap g\in\mathfrak{B}\{x: x\in X,\ g(x)=0\}$. THEOREM. *A function $\phi\in\mathfrak{C}(X)$ is arbitrarily closely uniformly approximable on X by functions g from $\mathfrak{P}$ if and only if there is a $g\in\mathfrak{P}$ such that $g(x)=\phi(x)$ for all $x\in J$. For $X=[-\alpha,\alpha](\alpha>0)$, and $\mathfrak{P}=$all polynomials with integral coefficients, and for certain other cases, the set J is identified explicitly.*

High school Mathematics Teaching (four fifteen-minute invited talks followed by discussion period):

1. *In-service programs for teachers*, by Miss Lesta Hoel, Supervisor of Mathematics, Portland Public Schools.

The emphasis in the in-service training program of mathematics teachers has changed from a consideration of *how* to teach to *what* to teach. The critical analysis of the past program and the investigation of what the program of the future should be has taken care of the "*how*." Colleges should plan more summer courses designed for teachers to fill in the gaps in their pre-service training. The product which the high school sends to the college is as strong as the teachers which the college trains. Mathematics education must be a cooperative project.

2. *What Portland does for the gifted child*, by Mr. Cecil Jenkins, Grant High School, Portland.

Special courses are offered for "exceptionally endowed" students in one section each of second year algebra (sophomores), plane and solid geometry (juniors), and trigonometry, advanced algebra (seniors). Student-participants in EE classes have high ratings in intelligence, academic ability and emotional maturity. Participants may apply through or be nominated by a teacher, counselor or the EE coordinator and must be approved by a committee. Class size of 10 to 15 may be raised to 25 to 30 next year. Grading is left to the teacher, but EE designation is removed from the transcript of a student receiving C or less in EE class. Extra funds are budgeted for books and instructional materials for EE classes. A teacher, chosen for subject matter competence, serves three years in the program.

3. *Reed College courses for teachers*, by Professor Burrowes Hunt, Reed College.

A brief description was given of the content of recent courses, primarily in-service courses or

summer workshops, for high school teachers. The emphasis has been on subjects directly relevant to high school courses: elementary number theory, rudiments of set theory and modern algebra, the nature of a deductive system, and basic properties of the real and complex number systems.

4. *The Meder Committee and pre-college mathematics*, by Professor J. M. Kingston, University of Washington.

The Commission on Mathematics of the College Entrance Examination Board believes that drastic revision of the content and point of view of high school mathematics is essential. Mathematics should not be presented as an accumulation of rules and tricks but rather the structure and pattern of mathematics should be emphasized. The Commission favors a gradual modification, modernization and improvement of existing curricula rather than any attempt at hasty replacement or improvisation. They have outlined a flexible four-year high school program consisting of two years of Elementary Mathematics, a third year of Intermediate Mathematics and a fourth year of Advanced Mathematics.

K. S. GHENT, *Secretary*

CALENDAR OF FUTURE MEETINGS

Forty-second Annual Meeting, University of Pennsylvania, Philadelphia, Pennsylvania, January 22–23, 1959.

Fortieth Summer Meeting, University of Utah, Salt Lake City, Utah, August 31–September 3, 1959.

The following is a list of the Sections of the Association with dates of future meetings so far as they have been reported to the Associate Secretary.

LLEGHENY MOUNTAIN, University of Pittsburgh, May 2, 1959.

ILLINOIS, Millikin University, Decatur, May 8–9, 1959.

INDIANA, Marian College, Indianapolis, November 7, 1958.

IOWA, State University of Iowa, Iowa City, October 17, 1958.

KANSAS

KENTUCKY, Centre College of Kentucky, Danville, April, 1959.

LOUISIANA-MISSISSIPPI, Buena Vista Hotel, Biloxi, Mississippi, February 13–14, 1959.

MARYLAND-DISTRICT OF COLUMBIA-VIRGINIA, George Washington University, Washington, D. C., December 6, 1958.

METROPOLITAN NEW YORK

MICHIGAN, Michigan State University of Agriculture and Applied Science, East Lansing, March 28, 1959.

MINNESOTA, University of Minnesota, Duluth, October 11, 1958.

MISSOURI, Lindenwood College, St. Charles, April 25, 1959.

NEBRASKA, University of Nebraska, Lincoln, April 18, 1959.

NEW JERSEY, Rutgers University, New Brunswick, November 1, 1958.

NORTHEASTERN, College of the Holy Cross, Worcester, Massachusetts, November 29, 1958.

NORTHERN CALIFORNIA, Stanford University, January 17, 1959.

OHIO

OKLAHOMA, Oklahoma City University, October 24, 1958.

PACIFIC NORTHWEST, University of Oregon, Eugene, June 19, 1959.

PHILADELPHIA, Lehigh University, Bethlehem, November 29, 1958.

ROCKY MOUNTAIN, Utah State University of Agriculture and Applied Science, Logan, Spring, 1959.

SOUTHEASTERN, East Tennessee State College, Johnson City, March 20–21, 1959.

SOUTHERN CALIFORNIA, University of Redlands, March 14, 1959.

SOUTHWESTERN, Arizona State College, Tempe, Spring, 1959.

TEXAS, University of Texas, Austin, April, 1959.

UPPER NEW YORK STATE, Hartwick College, Oneonta, May 9, 1959.

WISCONSIN, Wisconsin State College, Platteville, May, 1959.

THE CARUS MATHEMATICAL MONOGRAPHS

These Monographs are a series of expository presentations intended to make topics in pure and applied mathematics accessible to teachers and students of mathematics and also to non-specialists and scientific workers in other fields.

The complete list of Carus Mathematical Monographs is:

No. 1. *Calculus of Variations,* by G. A. Bliss. 1925.

No. 2. *Analytic Functions of a Complex Variable,* by D. R. Curtiss. 1926.

No. 3. *Mathematical Statistics,* by H. L. Rietz. 1927.

No. 4. *Projective Geometry,* by J. W. Young. 1930.

No. 5. *History of Mathematics in America before 1900,* by D. E. Smith and Jekuthiel Ginsburg. 1934. (Out of print)

No. 6. *Fourier Series and Orthogonal Polynomials,* by Dunham Jackson. 1941.

No. 7. *Vectors and Matrices,* by C. C. MacDuffee. 1943.

No. 8. *Rings and Ideals,* by N. H. McCoy. 1948.

No. 9. *The Theory of Algebraic Numbers,* by Harry Pollard. 1950.

No. 10. *The Arithmetic Theory of Quadratic Forms,* by B. W. Jones. 1950.

No. 11. *Irrational Numbers,* by Ivan Niven. 1956.

One copy of each monograph may be purchased by members of the Association for $1.75 per copy. Orders should be sent to Harry M. Gehman, Secretary-Treasurer, Mathematical Association of America, University of Buffalo, Buffalo, 14, New York.

Additional copies and copies for non-members of Monographs 1-8 are priced at $3.00 each, and must be purchased from the Open Court Publishing Co., LaSalle, Illinois.

In the case of Monographs 9-11, additional copies and copies for non-members must be purchased at $3.00 from John Wiley and Sons, 440 Fourth Ave., New York 16, New York.

MATHEMATICIANS

jpl

The Jet Propulsion Laboratory

now has opportunities open for Ph.D. Mathematicians of U.S. Citizenship to participate in many challenging problems relating to all phases of jet propulsion, aerodynamics, missile control and satellite flight.

Positions involve assignments in mathematical analysis, research in numerical analysis and consultation in applied mathematics. Computer facilities include an IBM-704 digital computer. Staff accommodations are excellent.

The laboratory is a continuing operation devoted to scientific research and development offering many opportunities for increasing responsibilities in an expanding activity.

JET PROPULSION LABORATORY
A DIVISION OF CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA • CALIFORNIA

The Slaught Memorial Papers

The Herbert Ellsworth Slaught Memorial Papers are a series of brief expository pamphlets (paper bound) published as supplements to the American Mathematical Monthly. The following numbers have been published recently:

3. *Proceedings of the Symposium on Special Topics in Applied Mathematics.* Nine articles by various authors. iv + 73 pages.

4. *Contributions to Geometry.* Eight articles by various authors. iv + 75 pages.

5. *The Conjugate Coordinate System for Plane Euclidean Geometry* by W. B. Carver. vi + 86 pages.

6. *To Lester R. Ford on His Seventieth Birthday.* A collection of fourteen articles. vi + 106 pages.

Copies at one dollar each postpaid may be ordered from:

HARRY M. GEHMAN, *Secretary-Treasurer*

MATHEMATICAL ASSOCIATION OF AMERICA
University of Buffalo
Buffalo 14, New York

Sourcebooks for the C.U.P.'s Basic Courses . . .

For the first college course (all qualified students):

1. UNIVERSAL MATHEMATICS

(A rearranged edition of *Universal Mathematics* Part I.) The basic one-semester course in "Graphs and Calculus." Analytic geometry (affine assumptions only); derivatives and integrals of polynomials; applications; calculus of exponential and logarithmic functions and general powers.

2. ELEMENTARY MATHEMATICS OF SETS—WITH APPLICATIONS

(A completely rewritten version of *Universal Mathematics* Part II.) This one-semester course is meant to foster intuitive command of the elementary language and techniques of sets. Natural numbers; combinatorial analysis; applications in simple mathematical models; elementary probability theory; basic descriptions of algebraic structures.

A special second course, designed chiefly for biology and social science majors:

MODERN MATHEMATICAL METHODS AND MODELS

3. M-4 Volume 1: MULTICOMPONENT MODELS

A one-semester course chiefly emphasizing algebra and analysis of functions of several variables. Vector spaces and matrix algebra; handbook techniques in calculus and in difference and differential equations; partial derivatives; convex functions; optimization problems with linear inequality constraints; applications to the social and biological sciences.

4. M-4 Volume II: MATHEMATICAL MODELS

Continuation of Volume I: Probability theory and Markov chains; order relations. Mathematical models: positive matrices; input-output models in economics; paired comparisons and associated orderings; sociological stratification theory; acceleration-multiplier model in economic theory (second order difference equation); the analogues differential equation for electric circuit theory. Theory of simple games.

Any interested person may get a FREE copy of any of these books by writing to

Professor H. M. Gehman
Mathematical Association of America
University of Buffalo
Buffalo 14, New York

COMMITTEE ON THE UNDERGRADUATE PROGRAM
MATHEMATICAL ASSOCIATION OF AMERICA

Now is the time to consider

these well recommended texts for your second semester courses . . .

"The best analytic geometry I have ever used"

McCOY & JOHNSON
Analytic Geometry 301 pp., $3.50

"One of the most teachable texts in this area . . . outstanding for teacher education."

EVES
An Introduction to the History of Mathematics 422 pp., $7.00

"Any teacher of engineering mathematics will enjoy this book."

MILLER
Engineering Mathematics 417 pp., $6.50

"A very remarkable book . . . excellent organization . . . impressive range of problems."

BEAUMONT & BALL
An Introduction to Modern Algebra and Matrix Theory 331 pp., $6.00

Rinehart & COMPANY, INC. • 232 MADISON AVE., NEW YORK 16, N. Y.

Now Ready

PROGRAMMING THE IBM 650

Magnetic Drum Computer and Data Processing Machine

by Richard V. Andree

Designed by an experienced teacher-author for classroom and laboratory use, this text offers numerous illustrative examples and problems which build a sound understanding of basic programming principles. Although the IBM 650 is used to provide operative codes and individual techniques, the principles taught apply to computers in general. Special attention is given to the type of "extra output data" which may be obtained "free," and to the elimination of costly "intermediate result punching" when it slows down the computer. Successfully used in semester courses, as well as in intensive short courses, this text has been acclaimed by both students and faculty members for its realistic approach to programming.

Henry Holt and Company

383 Madison Avenue, New York 17, N. Y.

Selected RONALD Books . . .

BASIC MATHEMATICS

H. S. Kaltenborn, Samuel A. Anderson, and Helen H. Kaltenborn
—all Memphis State University

This new, teachable book is designed to give freshmen a sound introduction to college mathematics. Assuming only a knowledge of arithmetic, this new textbook stresses fundamental principles and a mastery of mechanical procedures. Explains each basic rule and includes general proofs when within the student's grasp at that stage of instruction. Contains the essentials of arithmetic, elementary and intermediate algebra; the theories and techniques of trigonometry, analytic geometry, and statistics. *"A fine book. The coverage of statistics is particularly good."* **W. N. Huff,** *University of Oklahoma. 74 ills., tables; 392 pp. Instructor's Manual available.*

SOLID GEOMETRY

Hugo Mandelbaum and Samuel Conte
—both Wayne State University

Modern mathematical thought applied to the teaching of elementary solid geometry. Textbook emphasizes understanding and application rather than axiomatics and systematic proofs of theorems. Presents concepts of projective geometry to break the limitations imposed by Euclidian geometry. Thus, cylinders and prisms, cones and pyramids are viewed as interrelated to each other by their mode of generation. Covers the relationships of points, lines, and planes, and the measurement of all the more common solids. *". . . the authors have given considerable dignity to a much neglected subject."* **Adrien L. Hess,** *Montana State College. 296 ills., tables; 261 pp.*

TRIGONOMETRY

Roy Dubisch, Fresno State College

Mirrors a conspicuous trend in the teaching of plane trigonometry by presenting trigonometric functions as functions of real numbers, with trigonometric functions of angles as a supporting topic. Book develops the concept of a function as a rule of correspondence between two sets of objects and emphasizes the distinction between a function and function value. *"Done with a care which indicates that the author has been teaching this course to students and has learned of their difficulties.* **Gerald B. Huff,** *University of Georgia. "Ideal for the student who intends to take more advanced work in mathematics."* **R. N. Van Arnam,** *Lehigh University.* With arc length protractor and scale. *119 ills., tables; 396 pp.*

THE RONALD PRESS COMPANY

15 East 26th Street, New York 10, New York

Life Insurance Rates REDUCED!

TIAA continues to be your best buy for family protection.

For example . . . .

a premium of $11.40 a month buys $20,000 of 10-Year Term Insurance for a man 33 years of age. The net premium, after annual dividend, averages only $7.16 monthly for this $20,000 policy, based upon the factors used in determining TIAA's 1958 dividend scale. Dividends, of course, are not guaranteed.

Any staff member of a college, university or private school is eligible to apply for the many low-cost plans available.

TIAA employs no agents. No one will call on you.

Ask for details

TEACHERS INSURANCE AND ANNUITY ASSOCIATION

TIAA
522 Fifth Ave.
New York 36, N.Y.

I'd like details on low-cost life insurance.

Date of Birth_____

Ages of Dependents_____

Name_____

Address_____

Employing Institution_____

F

LINEAR PROGRAMMING: Methods and Applications

By SAUL I. GASS, Graduate School, U.S. Department of Agriculture. 223 pages, $6.50

This excellent introductory text presents the theoretical, computational, and applied areas of linear programming—explaining the problems it can solve and the implementing of techniques to formulate and solve them. It covers the revised simplex method, parametric linear programming, and a summary of digital computer codes.

COMPUTABILITY and UNSOLVABILITY

By MARTTIN DAVIS, Rensselaer Polytechnic Institute. *McGraw-Hill Series in Information Processing and Computers.* 214 pages, $7.50

Concerned with the existence of algorithms or effective computation procedures for solving various problems. It deals with the general theory of computability and the application of the subject to algebra, number theory, and symbolic logic. Here is the first connected presentation of this theory offered from the point of view of Turing machines.

MATHEMATICS OF PHYSICS AND MODERN ENGINEERING

By IVAN S. SOKOLNIKOFF and R. M. REDHEFFER, both at the University of California, Los Angeles. 810 pages, $9.50

Stresses those aspects which make mathematics a living and developing discipline. The need for rigor is emphasized by carefully motivated examples and counterexamples. A great variety of unique and up-to-date topics are included, i.e.: the comparison theorems for first-order differential equations, and mean and ordinary convergence of Fourier series.

ADVANCED CALCULUS

By R. CREIGHTON BUCK, University of Wisconsin. *International Series in Pure and Applied Mathematics.* 432 pages, $8.50

An excellent text for math majors, presupposing mastery of basic calculus and some differential equations. It gives a systematic and modern approach to the differential and integral calculus of functions and transformations, and develops analytical techniques for attacking some of the typical problems which arise in applications of mathematics. Includes 450 exercises.

Send for copies on approval

McGraw-Hill Book Company, Inc.

330 West 42nd Street New York 36, N.Y.

FUNDAMENTALS OF MATHEMATICS

Revised Edition

by Moses Richardson, Professor of Mathematics, Brooklyn College

Revised to include new mathematical development in the direction of the social sciences, this text gives the liberal arts student an insight into both the cultural and practical significance of mathematics. The basic concepts and applications of mathematics, rather than its formal technique, are stressed.

1958 507 pages $6.50

ELEMENTARY DIFFERENTIAL EQUATIONS

Revised Edition

by Earl D. Rainville, Professor of Mathematics, University of Michigan

This text, designed for students who have completed a course in calculus, aims at helping the student acquire a sound knowledge of elementary differential equations as well as correct techniques for solving equations. Emphasis is on the careful development and execution of solutions, particularly power series and Fourier series methods.

1958 449 pages $5.50

A SHORT COURSE IN DIFFERENTIAL EQUATIONS

Revised Edition

by Earl D. Rainville

Consisting of the first seventeen chapters of Rainville's *Elementary Differential Equations,* this text provides approximately 1,250 carefully constructed exercises, all accompanied by answers.

1958 259 pages $4.50

ARITHMETIC FOR COLLEGES

Revised Edition

by Harold D. Larsen, Professor and Head of the Department of Mathematics, Albion College

A comprehensive analysis of the theory and practice of arithmetic, this book is designed for prospective elementary school teachers. The text is enlivened by interesting historical notes and many amusing applications of arithmetic, such as puzzles and number forms.

1958 286 pages $5.50

PROBABILITY, STATISTICS AND TRUTH

by Richard von Mises

Second Revised English Edition prepared by Hilda Geiringer

Widely accepted as one of the outstanding works on statistics, this learned analysis has been revised to include a great deal of significant new material. The text emphasizes the possibility of arriving at reliable conclusions from statistical observations.

1957 244 pages $5.00

The Macmillan Company 60 Fifth Avenue New York 11, N.Y.

GEORGE BANTA COMPANY, INC., MENASHA, WISCONSIN, U.S.A.

TECHNOLOGY DEPT.

THE AMERICAN MATHEMATICAL MONTHLY

THE OFFICIAL JOURNAL OF
THE MATHEMATICAL ASSOCIATION OF AMERICA, INC.

VOLUME 65 NUMBER 8

PART II

Introduction to Arithmetic Factorization and Congruences from the Standpoint of Abstract Algebra

H. S. VANDIVER and MILO W. WEAVER

PUBLIC LIBRARY
OCT 31 1958
DETROIT

Number 7
of the
HERBERT ELLSWORTH SLAUGHT
MEMORIAL PAPERS

OCTOBER 1958

ONE DOLLAR A COPY

The AMERICAN MATHEMATICAL MONTHLY

(Founded in 1894 by Benjamin F. Finkel)

Ralph D. James, *Editor*

ASSOCIATE EDITORS

RICHARD V. ANDREE	G. E. HAY	C. O. OAKLEY
JOHN A. BROWN	L. M. KELLY	J. M. H. OLMSTED
ROY DUBISCH	JOHN R. MAYOR	E. P. STARKE
HOWARD EVES	LLOYD J. MONTZINGO, JR.	H. S. ZUCKERMAN
	IVAN NIVEN	

EDITORIAL CORRESPONDENCE should be addressed to the Editor, R. D. James, Department of Mathematics, University of British Columbia, Vancouver 8, Canada. Articles should be typewritten and double-spaced on 8½ by 11 paper. The greatest possible care should be taken in preparing the manuscript and authors should keep a complete copy.

ADVERTISING CORRESPONDENCE should be addressed to F. R. Olson, Mathematical Association of America, University of Buffalo, Buffalo 14, N.Y.

NOTICE OF CHANGE OF ADDRESS by members of the Association as well as correspondence regarding subscriptions to the Monthly should be sent to the Secretary-Treasurer, H. M. Gehman, Mathematical Association of America, University of Buffalo, Buffalo 14, N. Y.

THIS IS THE OFFICIAL JOURNAL OF THE

MATHEMATICAL ASSOCIATION OF AMERICA, INC.

(Devoted to the Interests of Collegiate Mathematics)

OFFICERS OF THE ASSOCIATION

President, G. B. Price, University of Kansas
First Vice-President, G. B. Thomas, Jr., Massachusetts Institute of Technology
Second Vice-President, B. W. Jones, University of Colorado
Secretary-Treasurer, H. M. Gehman, University of Buffalo
Associate Secretary, Lloyd J. Montzingo, Jr., University of Buffalo
Editor, R. D. James, University of British Columbia

Additional Members of the Board of Governors: H. M. Bacon, Jewell H. Bushey, Lamberto Cesari, H. S. M. Coxeter, P. H. Daus, W. L. Duren, Jr., H. P. Evans, Howard Eves, William Feller, N. J. Fine, J. S. Frame, A. S. Householder, G. B. Huff, W. N. Huff, G. K. Kalisch, E. C. Kiefer, J. C. Knipp, W. G. Leavitt, Z. L. Loflin, A. T. Lonseth, Saunders MacLane, J. R. Mayor, E. J. McShane, G. M. Merriman, R. S. Park, George Pólya, O. J. Ramler, C. R. Sherer, M. F. Smiley, R. G. Smith, B. M. Stewart, F. M. Stewart, W. R. Utz, Jr., Bernard Vinograde, Charles Wexler, C. R. Wylie, Jr.

Annual dues for members of the Association (including a subscription to the American Mathematical Monthly) are $5.00. For non-members the subscription price is $6.00.

Published by the Association at Menasha, Wisconsin, and Buffalo, N. Y., during the months of January, February, March, April, May, June-July, August-September, October, November, December.

Entered as second class matter at the post office at Menasha, Wis. Acceptance for mailing at special rate of postage provided for in the Act of February 28, 1925, embodied in Paragraph 4, Section 538, P. L. and R., authorized April 1, 1926.

PRINTED IN THE UNITED STATES OF AMERICA

INTRODUCTION TO ARITHMETIC FACTORIZATION AND CONGRUENCES FROM THE STANDPOINT OF ABSTRACT ALGEBRA

By

H. S. VANDIVER, *Professor of Mathematics*

and

MILO W. WEAVER, *Assistant Professor of Mathematics*

The University of Texas

The Seventh

HERBERT ELLSWORTH SLAUGHT

MEMORIAL PAPER

Published as a supplement to the AMERICAN MATHEMATICAL MONTHLY

Volume 65 Number 8

October, 1958

TABLE OF CONTENTS

CHAPTER		PAGE
	Introduction	1
I.	*Associative algebraic systems*	5
	1.1. Some references to associative algebra	5
	1.2. Some definitions	5
	1.3. Three theorems on semigroups	6
II.	*Semigroups with a unique basis, and primes*	8
	2.1. General uniquely factorable semigroups	8
	2.2. Unique factorization in the multiplicative semigroup of natural numbers	8
III.	*Ideals and congruences in the ring of rational integers*	12
	3.1. Principal ideals involving the rational integers	12
	3.2. Elements of arithmetic congruence theory	12
	3.3. An algorithm for a solution of a linear congruence	14
IV.	*The ring of residue classes modulo m*	17
	4.1. Residue classes	17
	4.2. An application of semigroups to a linear congruence	17
	4.3. Absolutely distinct solutions of polynomial equations in commutative rings	17
	4.4. A theorem on the product of the distinct elements of a finite Abelian group	18
V.	*The additive group of the ring of residue classes modulo m*	20
	5.1. On the generators of cyclic groups with application to the additive group modulo m	20
	5.2. Simple properties of the totient	22
VI.	*The multiplicative group $\mathfrak{G}(m)$ of residue classes C_a modulo m; $(a, m)=1$*	24
	6.1. The theorems of Euler and Wilson	24
	6.2. Criterion for the solution of a quadratic congruence modulo p	25
	6.3. The Minkowski-Thue theorem on linear congruences	25
	6.4. The expression of $p=4n+1$ as the sum of two squares	26
	6.5. Repetitive sets with application to Euler's theorem	26
	6.6. A basis theorem for finite Abelian groups	27
	6.7. A criterion for cyclic groups	29
	6.8. The number of solutions of $ax\equiv b \pmod m$, $(a, m)=d$, with application to cyclic groups	30
	6.9. Primitive roots modulo m	31
	6.10. A theorem on the cyclic subgroup of $\mathfrak{G}(m)$ of maximal order, with application to Carmichael numbers	34
	6.11. Integral homogeneous symmetric functions defined over repetitive sets in commutative rings with units	36
	6.12. Direct product of semigroups with application to $\mathfrak{G}(m)$	37

VII. *Quadratic reciprocity* 42
7.1. Simple properties of the Legendre symbol 42
7.2. Gauss' lemma 43
7.3. The law of quadratic reciprocity 44
VIII. *The semigroup of the nonunits of the multiplicative semigroup of residue classes modulo m* 48
8.1. On the groups contained in finite cyclic semigroups . . . 48
8.2. The cyclic semigroups generated by nonunit residue classes . 48
8.3. Unique factorization modulo *m* 49
IX. *The semiring formed by certain generalized residue classes* 52
9.1. Some finite commutative semirings 52
9.2. The generalized residue classes 53

INTRODUCTION

In the present paper* we discuss the beginnings of the theories of factorization and congruences, involving rational integers, using some of the simplest concepts in the theories of commutative semigroups (in particular, Abelian groups) and commutative rings. (As an example of the simplicity of the tools used, we nowhere employ the general basis theorem for Abelian groups.) In the main, we develop only those special results from semigroup or group theory that we find necessary in order to obtain our number theoretic results. We thereby obtain much more coherence in our account than has been apparent to us in expositions we have observed, published before this, in which nothing but elementary algebra was employed by the writers.

Up to the point where we introduce the concept of products of semigroups, at least, we hope this account will be understood by readers who have had little more than a first course in number theory or modern algebra. However, the remainder of the article is more sophisticated and may appeal mostly to experienced mathematicians.

As far as previous efforts to apply abstract algebra to number theory are concerned, we note that H. Weber† made some steps in this direction. For example, he treated the set of residue classes modulo m, using the term *Zahlklassen nach einem Modul*, by applying some elementary results in group theory. G. A. Miller‡ also obtained Fermat's and Wilson's theorems as well as several other elementary results by the use of simple properties of groups, and in particular of cyclic groups. Vandiver§ treated the theory of finite rings and semirings from a standpoint of developing results with direct application to number theory. In his courses in algebra and number theory at The University of Texas, he adopted the viewpoint of abstract algebra and group theory in discussing even

* About one-third of Vandiver's work on this paper was done under a Senior Postdoctoral Fellowship awarded to him by the National Science Foundation, and about two-thirds of the work done by Vandiver and about two-thirds of the work done by Weaver on this article was done under Basic Research Grant 3697, which was awarded to them by the National Science Foundation.

The writers wish to express their thanks to R. D. Allentharp who examined the manuscript with great care and made a number of valuable suggestions.

† Lehrbuch der Algebra, Bd. 2, Zweite Auflage, Braunschweig, Friedrich Vieweg und Sohn, vol. 60–68, 1899, pp. 302–314. On page 60 Weber remarks, "Das Wichtigste Beispiel einer endlichen commutativen Gruppe bieten die Reste der natürlichen Zahlen nach einem beliebeigen Modul, wenn sie durch die gewöhnliche Multiplication mit einander verbunden werden." Weber meant to limit himself here to residues prime to the modulus, as otherwise the residues modulo m do not, in general, form a group.

‡ Annals of Math. II, vol. 4, 1903, pp. 188–190; this MONTHLY, vol. 12, 1905, pp. 41–43; this MONTHLY, vol. 18, 1911, pp. 204–209.

§ Trans. Amer. Math Soc., vol. 13, 1912, pp. 293–304; Annals of Math., II, vol. 18, 1917, pp. 105–114; Proc. Nat. Acad. Sci., vol. 20, 1934, pp. 579–584; Bull. Amer. Math. Soc., vol. 40, 1934, pp. 914–920; Proc. Nat. Acad. Sci., vol. 21, 1935, pp. 162–165; Proc. Nat. Acad. Sci., vol. 23, 1937, pp. 552–555; this MONTHLY, vol. 46, 1939, pp. 22–26; Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, vol. 85, 1940, pp. 71–86; Annals of Math., II, vol. 48, 1947, pp. 22–28.

the most elementary parts of number theory. This point of view gradually developed in a period of some 25 years. In addition to this, Weaver‖ further developed these ideas in his classes at The University of Texas during the last five years and published some of the results obtained therefrom.

R. Fueter¶ applied some of the ideas of abstract algebra, including modules and ideals, as well as groups, in connection with a development of elementary number theory. He also employed such tools in a treatment of the theory of cyclotomic fields.

E. Hecke* gave an exposition of a considerable part of the theory of Abelian groups and applied the results to the elementary theory of numbers as well as to parts of the theory of algebraic numbers.

H. Hasse† considered the ring of residue classes modulo m and applied elementary group theory and ring theory to developing its properties. He assumed the properties of Abelian groups without proofs for his applications to the theory of the ring mentioned. Later he‡ again considered the ring of residue classes modulo m and used less of group theory than formerly, but he explained results he obtained by arithmetical methods, in terms of groups.

Now, under multiplication, the nonzero elements of the ring of residue classes form a semigroup which is not always a group. Aside from the authors of the present paper, however, none of the investigators above mentioned used semigroups in their accounts of elementary number theory. Also none of them considered the non-unit elements in the ring of residue classes modulo m where matters appear quite complicated unless some of the theory of semigroups is employed. The use of that system, and the introduction of possibly new concepts concerning it, with applications to factorization problems, in our opinion, constitutes the most novel part of our treatment. However, in parts of number theory where addition and multiplication are both involved in certain ways, the theory of semigroups is of little or no value, as in the theory of continued fractions, which we do not discuss here.

It may be that a reader of this paper is mainly interested in the number theoretical phase of it and may be of the opinion that it would have been much simpler to develop what we did here in the theory of congruences, directly, without the use of abstract algebra. However, most of the tools we have set up from the latter theory may be applied extensively, with little or no change, in the theories of finite fields, finite rings, and algebraic numbers. In fact, in writing this paper we have had, among other ideas, this end in view. Obviously, a purely arithmetic approach could not achieve this.§

‖ Math. Mag., vol. 25, 1952, pp. 125–136; this MONTHLY, vol. 63, 1956, pp. 387–391.

¶ Synthetische Zahlentheorie, Dritte Auflage, Walter de Gruyter and Co., Berlin, 1950.

* Vorlesungen über die Theorie der Algebraischen Zahlen, Akademische Verlagsgesellschaft, Leipzig, 1923.

† Zahlentheorie, Akademie-Verlag Berlin, 1949.

‡ Vorlesungen über Zahlentheorie, Springer-Verlag, Berlin, Göttingen, Heidelberg, 1950.

§ We note also that the article contains a considerable number of definitions, some of which are used very little. However, in further developments of the present ideas it would be very convenient to use them often.

The literature on elementary number theory is, of course, immense, and the literature on abstract algebra, particularly groups and their generalizations, likewise. Consequently, when we make references in this paper to the work of some other author on some particular idea, *this does not mean that we necessarily regard him as the first mathematician who published such an idea. The reference is given so that the reader might be able, because of it, to augment his knowledge of the topic being discussed.* If some reader thinks it would have been particularly illuminating to have referred to the work of some author we did not mention, we might be able to list such references in a supplement to the present article, if we are advised of these important omissions.

Of course, as time goes on, and particularly recently, more and more applications of modern algebra are being made to various parts of mathematics, pure and applied. The present contribution, of course, comes under the heading of an application to number theory.

Starting with a set of axioms for ordinary algebra and some consequences from them in the results given in section 1.1 below, the present article, we think, is self-contained in reference both to abstract algebra and number theory, aside from solution of the problems. The results we needed from abstract algebra in order to develop theorems in number theory are introduced in the text as we needed them, including the necessary definitions. Even aside from the algebraic approach, the proofs of the theorems we give often seem to contain elements of novelty.

The proofs of Theorems 6.9.12 and 6.12.14 are not simple. This has been also true of all other treatments of these topics we have noted elsewhere, and the difficulties seem to be inherent in the nature of the subjects.

Chapter I

ASSOCIATIVE ALGEBRAIC SYSTEMS

1.1. Some references to associative algebra. We have already treated the foundations of associative algebra, which include the foundations of the theory of integers, in four papers published in *Mathematics Magazine*, each under the title *A development of associative algebra and an algebraic theory of numbers*, appearing as follows:

(I)—Vandiver, vol. 25, 1952, pp. 233–250.
(II)—Vandiver, vol. 27, 1953, pp. 1–18.
(III)—Vandiver and Weaver, vol. 29, 1956, pp. 135–149.
(IV)—Vandiver and Weaver, vol. 30, 1956, pp. 1–8; Errata, vol. 30, 1957, p. 219.

In view of this, our present account will be naïve, but we shall give definitions and proofs in a form we think is usually acceptable in present-day number theory and algebra.

1.2. Some definitions. A *semigroup* $\mathfrak{S}$ is an algebraic system with *operation* $(\cdot)$ and *equivalence* $(=)$ such that for each $A, B, C \in \mathfrak{S}$, $A \cdot B = X$ has a unique solution $X \in \mathfrak{S}$, and $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. The operation symbol is usually omitted between elements of $\mathfrak{S}$. If $\mathfrak{S}$ has an element E such that for each $A \in \mathfrak{S}$, $AE = EA = A$, then E is called the *identity* of $\mathfrak{S}$. It is unique. If for each $A_1, A_2 \in \mathfrak{S}$, $A_1A_2 = A_2A_1$, $\mathfrak{S}$ is called *commutative* or *Abelian*.

If a semigroup $\mathfrak{G}$ has an identity E, and for each $B \in \mathfrak{G}$, the equations $BX = E$ and $YB = E$ have solutions, $X, Y \in \mathfrak{G}$, then it is easy to show that $X = Y$, and $\mathfrak{G}$ is called a *group*. It follows easily that X is unique, and it is called the *inverse* of B and is denoted by B^{-1}. If an element U in a semigroup $\mathfrak{S}$ has an inverse, U is called a *unit* in $\mathfrak{S}$. If $A_1A_2 \cdots A_n = C$, then the A's are *divisors* or *factors* of C, where C and the A's are in $\mathfrak{S}$. If $n \geqq 1$, then C is called a product of the A's.

The *order* of a semigroup $\mathfrak{S}$ is the number of distinct elements of $\mathfrak{S}$. If $A \in \mathfrak{S}$, the set of nonequivalent powers of A forms a *cyclic* semigroup $\mathfrak{C}$, and A is said to be a *generator* of $\mathfrak{C}$. If $\mathfrak{C}$ is finite, it contains a maximal subgroup $\mathfrak{G}$ which is also cyclic.* The orders of $\mathfrak{C}$ and $\mathfrak{G}$ are called, respectively, the *order* and *period* of A.

Let $\mathfrak{S}$ be a set with equivalence $(=)$ and operations addition $(+)$ and multiplication $(\times)$ (the latter sign is usually omitted) such that

* *Cf.* relation (8.1.2) that follows.

(i) $\mathfrak{S}$ is a semigroup relative to $+$ and $=$.
(ii) $\mathfrak{S}$ is a semigroup relative to $\times$ and $=$.
(iii) Whenever S_1, S_2, $S_3 \in \mathfrak{S}$, then $S_1(S_2+S_3)=S_1S_2+S_1S_3$, and $(S_2+S_3)S_1 = S_2S_1+S_3S_1$.
(iv) Substitution† as in ordinary arithmetic holds in $\mathfrak{S}$.

Under these conditions $\mathfrak{S}$ is called a *semiring*. The set of units, if there are any, of the multiplicative semigroup is called the set of *units* of the semiring. A semiring, whose additive semigroup (ASG) is a commutative group, is called a *ring*. The additive identity of a ring is denoted by 0. Suppose there is a ring $\mathfrak{R}$ whose multiplicative semigroup (MSG), the additive identity excluded, forms a commutative group. Such a ring is called a *field*.

The additive inverse of A, if it exists, in a semiring is denoted by $-A$; $A-B$ is used interchangeably with $A+(-B)$.

Let $\mathfrak{I}$ be a non-empty subset of a ring $\mathfrak{R}$ such that for any I_1, $I_2 \in \mathfrak{I}$ and $R \in \mathfrak{R}$, $I_1-I_2 \in \mathfrak{I}$, $RI_1 \in \mathfrak{I}$, and $I_1R \in \mathfrak{I}$; then $\mathfrak{I}$ is called an *ideal* of $\mathfrak{R}$. It is clear that $\mathfrak{I}$ is a subring of $\mathfrak{R}$, since $I_1-I_1=0$, $-I_1=0-I_1$, and $I_1-(-I_2)$ are also in $\mathfrak{I}$. Ideals have been extensively studied and have proved valuable in obtaining the structure of algebras. Hereafter in this paper we shall use small Greek letters to denote elements of a semiring except for semirings of rational integers.

We shall now give some examples of the concepts defined above. The sets will be taken from the set of rational numbers. As for semigroups, such examples are common. Let m be a positive integer; then the set of all positive multiples of m forms a semigroup under addition and also under multiplication. Under addition, the set mk with k ranging over all integers forms a group. However, the set of rational numbers, not including zero, forms a group under multiplication.

Perhaps the simplest example of a semiring is the set of natural numbers. The set of all positive multiples of a positive integer m also forms a semiring.

If a natural number m is multiplied by each integer we obtain a ring. The set of rational numbers forms a field.

If a and b are given integers, then the set $ax+by$ with both x and y ranging independently over the set of integers satisfies the conditions in our definition of an ideal in the ring of integers.

1.3. Three theorems on semigroups. We shall prove some theorems from group theory which we shall need several times.

If $\mathfrak{S}$ is a semigroup, $\mathfrak{R}: R_1, R_2, \cdots$ is a subset, finite or infinite, of $\mathfrak{S}$, and $S \in \mathfrak{S}$, we denote by $S\mathfrak{R}$, the set SR_i, $i=1, 2, \cdots$.

THEOREM 1.3.1. *If $\mathfrak{G}$ is a group of order n and $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$ of order d, then d divides n. If A generates a cyclic group $\mathfrak{G}$ of order n and $A^r=E$, where E is the identity of $\mathfrak{G}$, then n divides r.*

† As there exist semirings in which addition is not commutative, the order of the terms should be preserved here.

The first part of Theorem 1.3.1 is due to Lagrange. To prove it we shall show that the distinct elements of $\mathfrak{G}$ are the elements of disjoint sets, each containing d elements: $\mathfrak{H}$, $G_2\mathfrak{H}$, $G_3\mathfrak{H}$, $\cdots$, $G_{n/d}\mathfrak{H}$. $\mathfrak{H}$ contains d elements by hypothesis. We select $G_2 \notin H$, if such exists. Then $G_2\mathfrak{H}$ contains d elements, since from $G_2H = G_2H'$, we have $G_2^{-1}G_2H = G_2^{-1}G_2H'$ and $EH = EH'$ and therefore $H = H'$. $G_2\mathfrak{H}$ and $\mathfrak{H}$ are disjoint; otherwise from $G_2H = H'$ we would have $G_2 \in \mathfrak{H}$. We select $G_3 \notin \mathfrak{H}$, $G_3 \notin G_2\mathfrak{H}$ if such exists and find, similarly to the above discussion, that $G_3\mathfrak{H}$ contains d elements, no one of which is in $\mathfrak{H}$. And no element of $G_3\mathfrak{H}$ is in $G_2\mathfrak{H}$; otherwise, we would have $G_3 \in G_2\mathfrak{H}$. Since $\mathfrak{G}$ is finite, $\mathfrak{G}$ is exhausted by a number n/d of such sets, and we have the first part of our theorem.

To prove the second statement of the theorem, we use Theorem 2.2.8 below, the proof of which is independent of Theorem 1.3.1, and write $r = bn + c$, $0 \leq c < n$ and find, if $c \neq 0$, $A^r = A^{bn}A^c = EA^c = A^c = E$, contrary to hypothesis that A has order n. Hence n divides r.

THEOREM 1.3.2. *A semigroup $\mathfrak{G}$ is a group if and only if the equations $AX = B$ and $YA = B$ have solutions X and Y in $\mathfrak{G}$, for each $A, B \in \mathfrak{G}$.*

To prove this, suppose $\mathfrak{G}$ is a group. Then $A^{-1}B$ and BA^{-1} are solutions, respectively, of $AX = B$ and $YA = B$. To prove the converse, we let $A, B \in \mathfrak{G}$ and E and X be solutions, respectively, of the equations $YA = A$ and $AX = B$. Then $EB = E(AX) = (EA)X = AX = B$. Similarly if E' and Y' are solutions, respectively, of $AX = A$ and $YA = B$, we have $BE' = (Y'A)E' = Y'(AE') = Y'A = B$. Hence, for B arbitrary we have $EB = BE' = B$. Whence we have the identity $EE' = E' = E$. And from the solvability of $AX = YA = E$, we have the existence of an inverse for each $A \in \mathfrak{G}$. Our Theorem 1.3.2 follows.

An element C of a semigroup $\mathfrak{S}$ is said to be *left* (*right*) *cancellable* provided that if $A, B \in \mathfrak{S}$ and $CA = CB$ ($AC = BC$), then $A = B$. A *cancellable element* is one which is both right and left cancellable. If all elements of $\mathfrak{S}$ are cancellable then $\mathfrak{S}$ is called a *cancellative semigroup.*

Now let $\mathfrak{S}_1$ be a finite semigroup and consist of the distinct elements

$$A_1, A_2, \cdots, A_k. \tag{1.3.3}$$

We have

THEOREM 1.3.4. *If C is left cancellable in $\mathfrak{S}_1$, the set*

$$CA_1, CA_2, \cdots, CA_k \tag{1.3.5}$$

is a permutation of (1.3.3). *Any finite cancellative semigroup is a group.*

The proof follows immediately from the fact that if $CA_i = CA_j$ and $i \neq j$, then $A_i = A_j$ since C is left cancellable, which is a contradiction. Hence the set (1.3.5) gives k distinct elements in $\mathfrak{S}_1$, which gives a permutation of the elements in (1.3.3). The second part of the theorem follows from our definition of cancellative semigroup and Theorem 1.3.2.

Chapter II

SEMIGROUPS WITH A UNIQUE BASIS, AND PRIMES

2.1. General uniquely factorable semigroups. If a semigroup $\mathfrak{S}$ contains an element P, not the identity of $\mathfrak{S}$, which has no divisor other than possibly itself and the identity, if it exists in $\mathfrak{S}$, then P is called a *prime in* $\mathfrak{S}$. Nonunits which are not primes are called *composites*. If a nonunit D of $\mathfrak{S}$ is expressed as a product of primes, this expression is called a *decomposition of D into primes*.

Now suppose that $\mathfrak{S}$ is commutative and contains an identity E and that $\mathfrak{S}$ further satisfies:*

(i) $\mathfrak{S}$ contains a subset $\mathfrak{P}$ of primes.

(ii) If $S \in \mathfrak{S}$, and $S \neq E$, then S has exactly one decomposition into primes, aside from the order of the primes.

Then $\mathfrak{S}$ is said to be a *uniquely factorable semigroup*, and the prime elements of $\mathfrak{S}$ are said to be *independent* and to form together with E a *basis* for $\mathfrak{S}$. We notice that $\mathfrak{S}$ is a cancellative semigroup; also $\mathfrak{S}$ is infinite, for it follows from (i) and (ii) that each non-E element of $\mathfrak{S}$ generates an infinite cyclic semigroup.

2.2. Unique factorization in the multiplicative semigroup of natural numbers. Let $\mathfrak{N}$ denote the set of natural numbers with multiplication as an operation and ordinary equality as the equivalence. It follows from (I) of the series of papers in the *Mathematics Magazine* mentioned earlier, that $\mathfrak{N}$ is a multiplicative cancellative semigroup. The ordinary primes of $\mathfrak{N}$ satisfy (i) above, by definition. We shall use the word *prime* henceforth in this section only to denote natural number primes.

We shall now prove that the *number of distinct primes in the multiplicative semigroup of natural numbers is infinite.* To establish this we consider a prime p, and we shall determine a prime greater than p. Let n be the product of the distinct primes less than or equal to p. If $n+1$ is prime, the result is proved. If it is composite, it may be expressed as a product of primes, *viz.*, $n+1 = p_1 p_2 \cdots p_s$. It is impossible for one of these p's to coincide with one of the primes less than or equal to p. For if so, then there is a p_i such that $1 = p_i m$, with m an integer, but $|p_i m| > 1$. Hence each $p_i > p$. We now consider

THEOREM 2.2.1. *The natural numbers form a uniquely factorable cancellative semigroup under multiplication which has a unique infinite basis consisting of the set of prime numbers, together with unity.*

Proof. If we have an $m > 1$, we may show that it can be expressed as the product of a finite number of prime factors; that is, the primes are the generators of the semigroup of natural numbers >1. If m is not prime, let $p_1 > 1$ be

* M. Ward, Annals of Math., II, vol. 36, 1935, pp. 36–39. A. H. Clifford, Annals of Math., II, vol. 39, 1938, pp. 594–610. The (ii) part of our definition prevents $\mathfrak{S}$ from having more than one unit. We shall later generalize the idea of unique factorization to apply to semigroups with more than one unit and also the idea of prime such that a prime times any unit is a prime.

the smallest divisor, not 1, of m. It is evidently prime. Write $m=p_1m_1$. If m_1 is prime, we have our expression; if not, let $m_1=p_2m_2$ with p_2 prime. This process cannot continue indefinitely since $p_i\geqq 2$ and $\prod_{i=1}^{k} p_i\geqq 2^k$, which is greater than m for k sufficiently large; *i.e.*, by the binomial theorem $2^m=(1+1)^m=1+m+t$, $t>0$; so $2^m>m$. Hence

$$m = p_1p_2 \cdots p_s,$$

where each p is prime, and s is some integer. Two decompositions $m=p_1p_2 \cdots p_s$ $=p_1'p_2' \cdots p_t'$ are said to be the same if and only if $s=t$ and the p's are a permutation of the (p')'s.

We shall now show that no element of $\mathfrak{N}$ has two factor decompositions in $\mathfrak{N}$ into primes. Assume the contrary and let n be the smallest positive integer which has two different decompositions into prime factors. We set

$$n = p_1p_2 \cdots p_s = q_1q_2 \cdots q_t,$$

where

$$p_i \neq q_j; \qquad i = 1, 2, \cdots, s; \qquad j = 1, 2, \cdots, t,$$

since otherwise we obtain by cancellation an integer

$$n' < n$$

which has two distinct decompositions into primes. Let $p_1>q_1$; the argument is similar for $p_1<q_1$. Let

$$k = (p_1 - q_1)p_2p_3 \cdots p_s = p_1p_2 \cdots p_s - q_1p_2p_3 \cdots p_s.$$

Obviously $0<k<n$. Hence by the definition of n we have

$$\begin{aligned} k &= q_1q_2 \cdots q_t - q_1p_2p_3 \cdots p_s \\ &= q_1(q_2 \cdots q_t - p_1p_3 \cdots p_s), \end{aligned}$$

but q_1 is distinct from any prime appearing in the decomposition obtained from the other form of k. This gives $k<n$, and having two different expressions as the product of primes, contradicts the assumption. Since we have proved previously that the number of primes is infinite, and obviously unity (which was not considered in the above argument) forms the only other basis element, this gives Theorem 2.2.1.

If $a>0$ and $b>0$ have no factor greater than 1 in common, then they are said to be *relatively prime* or *prime to each other*. The *greatest common divisor* of two positive integers a and m will be designated henceforth as (a, m). In the statements 2.2.1–2.2.5 inclusive, the small letters employed will represent positive integers.

Problem 2.2.2. If n is arbitrary, show how to determine n consecutive composites.

The following corollaries follow immediately from Theorem 2.2.1.

COROLLARY 2.2.3. *If a and b are relatively prime and if ak is divisible by b, then k is divisible by b.*

COROLLARY 2.2.4. *If several positive integers are each prime to a, their product is prime to a.*

Problem 2.2.5. Show that if $m>0$ is not the kth power of a positive integer, then m is not the kth power of a rational fraction.

Problem 2.2.6. In a certain text it is argued that a special case $m=2$, $k=2$ of the last result may be proved without use of Theorem 2.2.1 because we cannot have two irreducible fractions equal with different numerators. Is this valid?

THEOREM 2.2.7 *If p is prime, the binomial coefficient*

$$\binom{p}{n}$$

is divisible by p, for $0<n<p$.

Proof. Since

$$\binom{p}{n} = \frac{p(p-1)\cdots(p-n+1)}{n!} = d,$$

an integer, then

$$p(p-1)\cdots(p-n+1) = n!d.$$

The decomposition of the left-hand member into prime factors contains p. On the right, the decomposition of $n!$ cannot contain p since each factor of it is less than p. Hence d is divisible by p.

We shall often need Theorem 2.2.8, below.

THEOREM 2.2.8. *If $a\neq 0$ and m are integers, unique integers r and q exist such that*

$$m = aq + r; \qquad 0 \leqq r < |a|. \tag{2.2.9}$$

We first use induction to prove this theorem for a and m both positive. If $m=1$, $a=1$, we have (2.2.9) with $q=1$, $r=0$. If $m=1$, $a>1$, we have (2.2.9) with $q=0$, $r=1$. Assume that (2.2.9) holds for $m=k>0$ and all $a>0$. Then $k+1=aq+r+1$. Since $0\leqq r<a$, either $0<r+1<a$ or $0<r+1=a$. If $r+1<a$, (2.2.9) is satisfied for $m=k+1$. If $r+1=a$, we have $k+1=a(q+1)+0$, and (2.2.9) holds with $r=0$; so our theorem holds for m, a both positive. If m is a multiple of a, solutions of (2.2.9) are obvious for all such m. Let $\bar{q}$, $\bar{r}$ be a solution of (2.2.9) for m', a', positive values of m, a. Then clearly if m is not a multiple

of a, we have, for the cases $m=-m'$, $a=-a'$; $m=-m'$, $a=a'$; $m=m'$, $a=-a'$; the solutions, respectively, of (2.2.9): $\bar{q}+1$, $a'-\bar{r}$; $-\bar{q}-1$, $a'-\bar{r}$; $-\bar{q}$, $\bar{r}$. Suppose that $m=aq_1+r_1=aq_2+r_2$ with $0\leqq r_1<|a|$, $0\leqq r_2<|a|$. Then $aq_1+r_1=aq_2+r_2$ and $r_1-r_2=a(q_2-q_1)$. Whence $r_1=r_2$, and r in (2.2.9) is unique. If $m=aq_1+r=aq_2+r$, we have $aq_1=aq_2$ and $q_1=q_2$.

Problem 2.2.10. Using the result of Theorem 2.2.8, we obtain for positive a_1 and a_2, $a_1>a_2$: $a_1=a_2q_1+a_3$, for $a_2>a_3\geqq 0$; $a_i=a_{i+1}q_i+a_{i+2}$, $a_i>a_{i+1}>a_{i+2}\geqq 0$ whence ultimately we have an n such that $a_n>0$, and $a_{n-1}=a_nq_{n-1}$. Show that a_n is (a_1, a_2). This is known as the *Euclidean Algorithm* for finding (a_1, a_2).

Chapter III

IDEALS AND CONGRUENCES IN THE RING OF RATIONAL INTEGERS

3.1. Principal ideals involving the rational integers. Now consider the subrings of the ring of rational integers $\mathfrak{R}$ and in particular the subrings which are ideals. Let $\mathfrak{I}$ be such an ideal and suppose that d is the smallest positive integer in it. Then by definition the ideal necessarily contains all integers in the form md where m ranges over all rational integers. Suppose the ideal contains an integer q different from any of these. By Theorem 2.2.8 we have $q=ad+r$, $0<r<d$. Now q belongs to our ideal and so does ad; consequently $q-ad=r$ belongs to the ideal, but $r<d$. This is a contradiction, however; consequently, *all the integers in the ideal have the form md, and the ideal is called principal.* Clearly if a and b are integers and h and k vary independently over the set of integers, the set $ah+bk$ is an ideal. Since this ideal is principal, if s is the smallest positive integer in it, it follows that there is a particular h_1 and k_1 such that

$$ah_1 + bk_1 = s. \tag{3.1.1}$$

3.2. Elements of arithmetic congruence theory. Due to the fact that in each of the ideals just considered each element may be put in the form ad, it is very convenient to use the concept of *congruence.* Thus we write

$$a \equiv b \pmod{m},$$

which reads "a is congruent to b modulo m," or $a=b$ plus some multiple of m. This is equivalent to the statement "a equals b plus an element in the ideal consisting of multiples of m." The sign $\not\equiv$ is read "is not congruent to," or "is incongruent to." All moduli will be assumed >1 unless we state otherwise.

Examples: $7\equiv 2 \pmod 5$; $-3\equiv 4 \pmod 7$; $15\equiv 0 \pmod 5$; $14\not\equiv 1 \pmod{11}$.

Unless it is otherwise stated, from now on all small Latin letters employed in connection with formulas will denote integers.

Using the definition of congruence we easily obtain a proof of

THEOREM 3.2.1. *If* $a\equiv b$ *and* $c\equiv d \pmod m$ *then* $a+c\equiv b+d \pmod m$ *and* $ac\equiv bd \pmod m$.

This theorem includes the result that if $a\equiv b \pmod m$ then $na\equiv nb \pmod m$.

But from the latter we cannot always conclude the former; thus

$$2 \times 4 \equiv 2 \times 1 \pmod 6, \text{ but } 4 \not\equiv 1 \pmod 6.$$

Here we extend the notion of "prime to" by defining n as prime to an integer k if and only if $|n|$ is prime to $|k|$, and similarly for the notion of "divisible by." We shall have occasion to employ frequently the result of

THEOREM 3.2.2. *If* $na \equiv nb \pmod m$ *and* n *is prime to* m, *then* $a \equiv b \pmod m$.

Proof. From the hypothesis, $n(a-b) = mr$, and since n is prime to m, we have $a-b$ divisible by m by using Corollary 2.2.3. Hence $a-b \equiv 0 \pmod m$ and $a \equiv b \pmod m$.

If $a \equiv r \pmod m$, then r is said to be a *residue* of a, modulo m. If $0 \leqq r < m$, then r is said to be the *least residue* of a modulo m.

Problem 3.2.3. If m is odd, show that any integer a is congruent to one of the integers $0, \pm 1, \pm 2, \cdots, \pm(m-1)/2$. This one is called the *least absolute residue* of a, modulo m.

Problem 3.2.4. Extend Theorem 3.2.2 to the case where n and m have the greatest common divisor d by restricting the modulus in the result.

We shall use Theorem 2.2.1 to obtain the following useful theorem.

THEOREM 3.2.5. *If* $a \equiv k \pmod{m_1}$ *and* $a \equiv k \pmod{m_2}$ *with* $(m_1, m_2) = 1$, *then* $a \equiv k \pmod{m_1 m_2}$.

Keeping Theorem 2.2.1 in mind, throughout the proof, we use the definition of congruence to obtain

$$a - k = m_1 h = m_2 j = p_1^{i_1} p_2^{i_2} \cdots p_c^{i_c}$$

with the p's relatively prime in pairs. Hence since $(m_1, m_2) = 1$, if we separate the prime divisors of m_1 from those of m_2 in the right of the above equation, we see that m_2 divides h by Corollary 2.2.3; so we may write $h = h_1 m_2$ and obtain $a - k = m_1 h_1 m_2$; whence

$$a \equiv k \pmod{m_1 m_2}.$$

3.3. An algorithm for a solution of a linear congruence. We shall now call attention to an algorithm* for the solution of the linear congruence 3.3.1 below. We shall be particularly interested in showing how to find, as briefly as possible, an x with $0<x<m$ such that with $b\not\equiv 0 \pmod{m}$,

$$ax \equiv b \pmod{m}, \tag{3.3.1}$$

a and m being positive integers such that $(a, m)=1$, with $0<a<m$.

---

* Said algorithm differs considerably from the well-known method depending on the expansion of m/a as a continued fraction, since contrary to the other method, it definitely belongs to the theory of congruences, at least in the case of a prime power modulus, and the theory behind the method which follows is far simpler. *Cf.* Vandiver, this MONTHLY, vol. 31, 1924, pp. 137–140. In setting up the algorithm in a particular case we note that we may select the k's so as to make the absolute values of the remainders as small as possible. For example, for the case $81x\equiv 1 \pmod{257}$, from

$$257 = 81 \times 3 + 14$$

we see that 81 is close to 6×14; so we use

$$\begin{aligned} 6 \times 257 &= 81 \times 19 + 3, \\ 257 &= 3 \times 86 - 1. \end{aligned}$$

Whence

$$\begin{aligned} 81(19 \times 86) &\equiv -1 \pmod{257}, \\ 81 \times 165 &\equiv 1 \pmod{257}. \end{aligned}$$

In our general argument we employed more than one modulus when the given modulus was not a power of a prime. However, by trial we can sometimes carry the work to a finish by using one modulus only. For example, consider

$$31x \equiv 1 \pmod{120}.$$

We have

$$\begin{aligned} 2\cdot 120 &= 7\cdot 31 + 23, \\ 2\cdot 120 &= 23\cdot 11 - 13, \\ 2\cdot 120 &= 13\cdot 19 - 7, \\ 120 &= 7\cdot 17 + 1. \end{aligned}$$

Hence

$$31(7\cdot 11\cdot 19\cdot 17) \equiv 1 \pmod{120}.$$

This example indicates that our main difficulties in connection with such a procedure are likely to appear when the modulus contains several small prime factors. As another problem of this type we investigate

$$1723x \equiv 1 \pmod{4028}.$$

Without setting down the actual figures, we see immediately that the remainder when 4028 is divided by 1723 is close to $\frac{1}{7}$ of 1723. Hence we set

$$\begin{aligned} 3\cdot 4028 &= 1723\cdot 7 + 23, \\ 4028 &= 23\cdot 175 + 3, \\ 4028 &= 3\cdot 1343 - 1; \end{aligned}$$

and we have

$$1723(7\cdot 175\cdot 1343) \equiv 1 \pmod{4028}.$$

Assume first that $m=p^n$, where p is prime and k_1 is an integer. We use Theorem 2.2.8 to obtain

$$k_1 m = aq_1' + r_1',$$

where k_1 is selected* so as not to be a multiple of a; and r_1' is selected so that it is the least absolute residue of $k_1 m$, modulo a. If, however, r_1' is divisible by p, put

$$k_1 m = a(q_1' \pm 1) + r_1' \mp a$$

according as r_1' is negative or positive; hence $|r_1' \mp a| < a$. Now $r_1' \mp a$ is prime to p, for if we assume $r_1' \mp a \equiv 0 \pmod{p}$, then $a \equiv 0 \pmod{p}$, contrary to hypothesis. Hence we may write, in any case,

$$k_1 m = aq_1 + r_1,$$

where $0 < |r_1| < a$, and r_1 is prime to p.

Similarly, after selecting an r_2 as a certain residue of $k_2 m$ modulo r_1, prime to p in the same manner that r_1 was selected as a certain residue of $k_1 m$, modulo a, and prime to p, we have

$$k_2 m = r_1 q_2 + r_2,$$

where $0 < |r_2| < |r_1|$ and r_2 is prime to m, k_2 being an integer $\not\equiv 0 \pmod{r_1}$. Proceeding in this way we obtain ultimately

$$k_s m = r_{s-1} q_s + r_s,$$

where $|r_s| = 1$. Hence in general we have

$$k_i m = r_{i-1} q_i + r_i,$$

$i = 1, 2, \cdots, s$, and $r_0 = a$, $|r_s| = 1$. Also k_i is an integer, $\not\equiv 0 \pmod{r_{i-1}}$, and r_i is prime to m.

We may then write

$$r_{i-1} q_i \equiv -r_i \pmod{m}.$$

Setting $i = 1, 2, \cdots, s$, and multiplying all the congruences together, we have by Theorem 3.2.1

$$a \prod_{i=1}^{s} q_i \prod_{c=1}^{s-1} r_c \equiv (-1)^s r_s \prod_{c=1}^{s-1} r_c \pmod{m}.$$

Using Theorem 3.2.2, since $\prod_{c=1}^{s-1} r_c$ is prime to m, we have

$$a \prod_{i=1}^{s} q_i \equiv (-1)^s r_s \pmod{m}.$$

* Vandiver, Proc. Nat. Acad. Sci., vol. 21, 1935, p. 163.

So, noting that $|r_s| = 1$, we have as a solution of (3.3.1)

$$x = (-1)^s b r_s \prod_{i=1}^{s} q_i. \tag{3.3.2}$$

For the case $m = p$, a prime, the algorithm takes a simple form since for $n = 1$ each r_i above is necessarily prime to p.

Consider (3.3.1) again with $m = m_1 m_2 \cdots m_t$; $m_i = p_i^{n_i}$; $i = 1, 2, \cdots, t$; $(m_i, m_j) = 1$, with i and j any pair of distinct integers in the set $1, 2, \cdots, t$. Further, write $h_i = m/p_i^{n_i}$, $i = 1, 2, \cdots, t$. Then by the above-described method we obtain $y_1, y_2, \cdots, y_t$, such that

$$(ah_i)y_i \equiv b \pmod{m_i},$$

$i = 1, 2, \cdots, t$. The quantity

$$x = h_1 y_1 + \cdots + h_t y_t \tag{3.3.3}$$

satisfies (3.3.1), as we see on using the result of Theorem 3.2.5. When we wish a solution from (3.3.2) or (3.3.4) with $0 < x < m$ in (3.3.1), we may reduce (3.3.2) or (3.3.3) modulo m.

Chapter IV

THE RING OF RESIDUE CLASSES MODULO m

4.1. Residue classes. We shall now define the notion of residue classes, modulo m. For a fixed integer $m>0$ we notice that the m sets defined by $a+km$ give the set of all integers where k ranges over all integers and a ranges independently over $0, 1, \cdots, m-1$. Corresponding, then, to each value of a, there is an infinite set of integers each congruent to a, modulo m, which set we shall denote by C_a, and we consider

$$C_0, C_1, \cdots, C_{m-1}, \tag{4.1.1}$$

which are mutually exclusive by Theorem 2.2.8. *With these definitions in mind, in the rest of this paper we shall pass freely from any equation involving the C_a's to a congruence, modulo m, in which C_a is replaced by a, and vice versa.* We postulate $C_a=C_b$ if C_a and C_b represent the same set. We also postulate $C_a+C_b=C_k$ where $0\leqq k<m$ whenever $a+b\equiv k \pmod m$. Similarly $C_aC_b=C_h$ where $0\leqq h<m$ whenever $ab\equiv h \pmod m$. Then these C's obviously form an Abelian group under addition, and an Abelian semigroup under multiplication. Also the distributive law and substitution hold. Consequently the C's form a ring, which is called *the ring of residue classes modulo m.*

4.2. An application of semigroups to a linear congruence. In applying the C's to obtaining arithmetical results we first consider the multiplicative semigroup formed by the elements of (4.1.1). Referring to the proof of Theorem 1.3.4, take the set (1.3.3) mentioned there and suppose it to be the set (4.1.1) above, and let the C of (1.3.5) be an element C_a of (4.1.1) with $(a, m)=1$. Then C_a is a cancellable element of (4.1.1), so that Theorem 1.3.4 gives the result

THEOREM 4.2.1. *The conditional congruence in x,*

$$ax \equiv b \pmod m; \qquad (a, m) = 1, \tag{4.2.2}$$

has a unique solution x, $0\leqq x<m$.

4.3. Absolutely distinct solutions of polynomial equations in commutative rings. We shall now apply a result in ring theory to congruence theory. Let $\mathfrak{R}$ be a commutative ring with a multiplicative identity, called a *unity* element. Two elements α and β in $\mathfrak{R}$ are said to be *absolutely distinct* if $\alpha-\beta$ is not zero and not a zero divisor. They are said to be *semi-equal* if $\alpha-\beta$ is a zero divisor, a *zero divisor* in $\mathfrak{R}$ being an element $\gamma\neq 0$, such that $\gamma\sigma=0$ with $\sigma\neq 0$. Also, if $h(x)$ is a polynomial with coefficients in $\mathfrak{R}$, a solution of $h(x)=0$ in $\mathfrak{R}$ is called a *zero* of $h(x)$ in $\mathfrak{R}$. We then have

THEOREM* 4.3.1. *The equation with* $\alpha_n \not\equiv 0$ (*said to be of degree* n)

$$\alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 = 0 \tag{4.3.2}$$

has no more than n *absolutely distinct roots in* $\mathfrak{R}$, *where* $\mathfrak{R}$ *is a commutative ring with a unity element, and the* α'*s are in* $\mathfrak{R}$ *with* $n>0$.

For a proof, suppose the statement not true and let k be the degree of a polynomial $f(x)$ of least degree with coefficients in $\mathfrak{R}$ for which the statement is not true. Obviously $k>1$. Let $\theta_1, \theta_2, \cdots, \theta_{k+1}$ be absolutely distinct zeros of $f(x)$ in $\mathfrak{R}$. By an easy extension of ordinary algebraic division we have the identity

$$f(x) = (x - \theta_1)g(x) + \gamma,$$

where γ is in $\mathfrak{R}$, and when we set $x=\theta_1$, this gives $\gamma=0$. The above relation shows that the leading coefficient of $g(x)$ is α_n, and $g(x)=0$ for $x=\theta_i$, $i=2, 3, \cdots, k+1$, since the θ's are absolutely distinct. But the degree of $g(x)$ is less than that of $f(x)$.

Two integers a and b are said to be *absolutely incongruent* modulo m if $a-b$ is prime to m. They are said to be *semi-congruent* modulo m if $a-b$ has a factor f in common with m, such that $m>f>1$.

If we now take $\mathfrak{R}$ to be the ring of residue classes modulo m in Theorem 4.3.1, we immediately derive the

COROLLARY 4.3.3. *The congruence with* $a_n \not\equiv 0 \pmod m$ (*said to be of degree* n)

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0 \pmod m \tag{4.3.4}$$

has no more than n *absolutely incongruent solutions in* x *modulo* m; $n>0$.

4.4. A theorem on the product of the distinct elements of a finite Abelian group. We shall now obtain a result (Theorem 4.4.9) concerning commutative groups which has considerable application to congruences.

Let $\mathfrak{G}$ be a commutative group of order $2n$. Let $A_1 \in \mathfrak{G}$. Then there exists an $A_1' \in \mathfrak{G}$ such that, if $M \in \mathfrak{G}$,

$$A_1 A_1' = M. \tag{4.4.1}$$

We will now consider an $A_2 \in \mathfrak{G}$ distinct from A_1 and A_1', if such an A_2 exists. As before, there exists an A_2', with $A_2' \in \mathfrak{G}$ such that

$$A_2 A_2' = M. \tag{4.4.2}$$

Clearly $A_1' \neq A_2'$, for assuming them equal yields $A_1=A_2$. Similarly $A_2' \neq A_1$. In this way we continue until the elements of $\mathfrak{G}$ are exhausted and obtain a set of r equations of the type (4.4.2). We shall now separate these into two classes, one class if not null containing only the relations of the type (4.4.2) in which A_i is distinct from A_i' so that we may write, after changing subscripts, if necessary,

* Vandiver, Proc. Nat. Acad. Sci., vol. 21, 1935, p. 163.

$$A_i A_i' = M, \tag{4.4.3}$$

$i=1, 2, \cdots, s$, and the other class, if not null, containing those of the A's such that

$$A_j^2 = M, \tag{4.4.4}$$

There are $2n-2s$ of these elements. Let $t=2n-2s$.

Let E be the identity of $\mathfrak{G}$. Then if we set $M=E$ in (4.4.3) and (4.4.4), and notice that elements of order >2 satisfy (4.4.3), and elements of order 1 or 2 satisfy (4.4.4), we see that $\mathfrak{G}$ has an odd number of elements of order 2, since E is the only element of order 1. Let H be one of them. Then we obtain from (4.4.4) an element A_{2s+1} such that

$$A_{2s+1}(A_{2s+1}H) = HM. \tag{4.4.5}$$

Now $A_{2s+1}H$ by definition of H is an element distinct from A_{2s+1}. Select an element A_{2s+2}, defined in (4.4.4), which is distinct from A_{2s+1} and $A_{2s+1}H$ if any such element exists. Then

$$A_{2s+2}(A_{2s+2}H) = HM. \tag{4.4.6}$$

Using the reasoning used above to establish (4.4.2), we see that $A_{2s+2}H \neq A_{2s+1}$, $A_{2s+2}H \neq A_{2s+1}H$, $A_{2s+2}H \neq A_{2s+2}$. In this way we continue until the elements thus obtained from (4.4.4) are exhausted, and we may then write

$$A_{2s+c}(A_{2s+c}H) = HM, \tag{4.4.7}$$

$c=1, 2, \cdots, k$, with each A_{2s+c} one of the A_j's in (4.4.4). In view of (4.4.3) and the way the A_j's were defined in (4.4.4), the two factors in the left-hand members of the relations (4.4.3) together with those in the left of (4.4.7) give each of the distinct elements of $\mathfrak{G}$ just once; that is, since $2k+2s=2n$, then $k=t/2$. Since $\mathfrak{G}$ is commutative we can then multiply together the s relations (4.4.3) and the relations (4.4.7), obtaining, if $B_1, B_2, \cdots, B_{2n}$ are the distinct elements of $\mathfrak{G}$,

$$\prod_{h=1}^{2n} B_h = M^n H^{t/2}. \tag{4.4.8}$$

In the above argument we excepted the cases where either of the classes was null. If the class (4.4.3) is null, then (4.4.8) holds also, since here $s=0$ and $t=2n$. If the class (4.4.4) is null, then (4.4.8) holds for $t=0$, with H^0 defined as E. We then have

THEOREM 4.4.9. *Let $\mathfrak{G}$ be a finite Abelian group of order $2n$; then the relation* (4.4.8) *holds with $t \geqq 0$. Here $B_1, B_2, \cdots, B_{2n}$ are the distinct elements of $\mathfrak{G}$; H is some element of order 2 in $\mathfrak{G}$, $M \in \mathfrak{G}$, and t is the number of elements A_j which satisfy* (4.4.4).

Chapter V

THE ADDITIVE GROUP OF THE RING OF RESIDUE CLASSES MODULO m

5.1. On the generators of cyclic groups with application to the additive group modulo m. As we noted in remarks made below our relation (4.1.1), the ASG of the ring of residue classes modulo m is an Abelian group. Also, this group $\mathfrak{F}(m)$ is obviously cyclic with one of its generators being C_1.

We shall now consider the subgroups of the general cyclic group and shall prove the useful

THEOREM 5.1.1. *A subgroup of a cyclic group $\mathfrak{C}$ of order n and generator A is cyclic of order d where d divides n, and corresponding to any such d there is a unique subgroup of $\mathfrak{C}$ of order d. If $A^{n/d}$ generates a cyclic subgroup of order d, then $A^{kn/d}$ is a generator if and only if k is prime to d.*

Let $\mathfrak{G}$ be a cyclic group of order n and generator A with E its identity element. We shall show first that any subgroup $\mathfrak{G}_1 \subset \mathfrak{G}$ of order d has the form

$$A^c, A^{2c}, \cdots, A^n = E \tag{5.1.2}$$

where $n/d = c$ and where c is the smallest integer such that $A^c \in \mathfrak{G}_1$. If $A^k \in \mathfrak{G}_1$ then $k = qc + r$ with $0 \leqq r < c$. Hence by Theorem 1.3.2, $A^r \in \mathfrak{G}_1$. If $r > 0$ this contradicts the definition of c. Hence $r = 0$; so all the elements of $\mathfrak{G}_1$ are of the form A^{tc}. Also $A^n = E$ so $A^n \in \mathfrak{G}_1$ which gives $n \equiv 0 \pmod{c}$. Hence if d divides n there is a cyclic subgroup of $\mathfrak{G}$ of order d. There cannot be another subgroup $\mathfrak{G}_2$ of order d since A^c is unique in $\mathfrak{G}_1$.

We now seek all the generators of (5.1.2). Let $(h, d) = t$, $h = h_1 t$, and $d = d_1 t$. Then, since $(A^c)^d = E$, we have $(A^{hc})^{d_1} = (A^c)^{h_1 t d_1} = (A^c)^{d h_1} = E^{h_1} = E$. Clearly if A^{hc} is a generator of $\mathfrak{G}_1$, $d_1 = d$ and $(h, d) = 1$. On the other hand, if $(h, d) = 1$ and A^{hc} has order r, $A^{chr} = E$, and, by Theorem 1.3.1, d divides hr and therefore r, by Corollary 2.2.3. By definition of *generator*, $d = r$ and A^{hc} is a generator of $\mathfrak{G}_1$ if $(h, d) = 1$. This gives the second statement in the Theorem.

If $rs = m$; $r > 1$, $s > 1$; with $(r, s) = 1$, then $\mathfrak{F}(m)$ can be represented as the *sum* of the two additive cyclic groups defined by C_{rk}; $k = 0, 1, \cdots, s-1$, and C_{sl}; $l = 0, 1, \cdots, r-1$; *that is, $C_{rk} + C_{sl}$ with k and l ranging as above give distinct elements which coincide with the elements of $\mathfrak{G}$.* (This additive notation for groups is described in more detail in section 6.6.) To prove this it is sufficient to show that the integers $rk + sl$, with k and l ranging as above, are congruent in some order to the integers $0, 1, \cdots, m-1$. In the first place, any integer a may be represented in this form, for by Theorem 4.2.1 it follows that there is an x and y such that

$$a = rx + sy, \tag{5.1.3}$$

and by Theorem 2.2.8 we may write $x=x_1+sq_1$, $0\leqq x_1<s$; $y=y_1+rq_2$, $0\leqq y_1<r$; which gives by substitution in (5.1.3),

$$c \equiv rx_1 + sy_1 \pmod{m}, \tag{5.1.4}$$

with x_1 in the range $0, 1, \cdots, s-1$, and y_1 in the range $0, 1, \cdots, r-1$. No two such representations modulo m coincide. For if we substitute x_2 in place of x_1, and y_2 in place of y_1, in (5.1.4), with the same restrictions on x_2 and y_2 as we placed on x_1 and y_1, respectively, then upon subtracting the resulting relation from (5.1.4), we have

$$r(x_1 - x_2) + s(y_1 - y_2) \equiv 0 \pmod{m};$$

whence

$$r(x_1 - x_2) \equiv 0 \pmod{s};$$

or since $(r, s)=1$, $x_1=x_2$. Similarly $y_1=y_2$, which proves the last result stated in italics above.

We shall now define a very important arithmetical function, corresponding to each positive integer m, known usually as *Euler's ϕ function* or the *indicator* or *totient* of m. It is defined as $\phi(m)=1$ for $m=1$ and as the number of integers less than m and prime to it for $m>1$.

Consider again the relation (5.1.4) with the conditions mentioned below it. Assume that for $0\leqq a<m$ there exist $u=x_1$ and $v=y_1$ such that $(u, s)=1$, $(v, r)=1$, and

$$ru + sv \equiv a \pmod{m}. \tag{5.1.5}$$

Then $(a, s)=1$, since from (5.1.5) $ru\equiv a \pmod{s}$, with $(r, s)=1$, $(u, s)=1$. Similarly $(a, r)=1$. Hence $(a, m)=1$. Conversely (5.1.5) for $(a, m)=1$ gives $(u, s)=1$, and $(v, r)=1$. For it gives $ru\equiv a \pmod{s}$, and, since $(r, s)=1$, $(u, s)=1$; similarly for r in place of s we obtain $(v, r)=1$. Also, there cannot be another such representation of a, modulo m in (5.1.5) since x_1 and y_1 are unique in (5.1.4).

If we consider the additive group $\mathfrak{F}(m)$ of residue classes modulo m and apply the result in (5.1.5) to the cyclic subgroups $\mathfrak{F}(r)$ and $\mathfrak{F}(s)$ of orders r and s respectively, then (5.1.5) gives the result that any generator of $\mathfrak{F}(m)$ can be expressed uniquely as the sum of a generator of $\mathfrak{F}(r)$ and a generator of $\mathfrak{F}(s)$. However, it is clear that any cyclic group whatever can be represented by means of an additive cyclic group of residue classes modulo m. In (5.1.5) we assumed that $r>1$ and $s>1$, but we now state a result which is also obviously true for $r=1$ or $s=1$, namely:

THEOREM 5.1.6. *Any generator of an additive cyclic group* $\mathfrak{F}(m)$ *of order* m *may be expressed uniquely as the sum of some generator of* $\mathfrak{F}(r)$ *and some generator of* $\mathfrak{F}(s)$ *where* $m=rs$, $(r, s)=1$, *and conversely the sum of a generator of* $\mathfrak{F}(r)$ *and one of* $\mathfrak{F}(s)$ *gives one of* $\mathfrak{F}(m)$, *no two distinct sums giving the same generator of* $\mathfrak{F}(m)$.

(Generalizations of Theorem 5.1.6 have led to a number of results in the theory of finite rings.)

5.2. Simple properties of the totient. From the above result we obtain, by counting the number of distinct generators in each of the groups mentioned, the

COROLLARY 5.2.1. *If* $m=rs$, $(r, s)=1$, *then*

$$\phi(m) = \phi(r)\phi(s). \tag{5.2.2}$$

If $m=p_1^{d_1}p_2^{d_2}\cdots p_t^{d_t}$ with the p's distinct primes, then by using (5.2.2) successively,

$$\phi(m) = \prod_{i=1}^{t} \phi(p_i^{d_i}). \tag{5.2.3}$$

Also, as is easily seen,

$$\phi(p_i^{d_i}) = p_i^{d_i-1}(p_i - 1), \tag{5.2.4}$$

and (5.2.3) and (5.2.4) give

THEOREM* 5.2.5. *We have, if* $m>1$,

$$\phi(m) = m\prod_{i=1}^{t} (1 - (1/p_i)), \tag{5.2.6}$$

where $p_1, p_2, \cdots, p_t$ *are the distinct prime divisors of* m.

---

* Euler gave a proof of the existence of an infinity of primes using Theorem 5.2.5: assume the number of primes is finite with p the greatest and set as the product of all the primes,

$$n = 2\cdot 3\cdot 5\cdots p.$$

Then we have

$$\phi(n) = (2-1)(3-1)\cdots(p-1),$$

which is a contradiction, since by definition of n, $\phi(n)=1$. So a prime p_1 must exist with $p<p_1<n$. This is slightly more general than the result obtained, from the usual proof, that $p<p_1<n+2$.

Let $\mathfrak{G}$ be a cyclic group of order n with a cyclic subgroup $\mathfrak{G}_1$ of order d where d divides n. $\mathfrak{G}_1$ exists and is unique by Theorem 5.1.1. Then by Theorem 5.1.2, $\mathfrak{G}_1$ has just $\phi(d)$ distinct generators. Also, any element of $\mathfrak{G}$ generates some cyclic group. Whence

THEOREM† 5.2.7. *We have*

$$\sum_d \phi(d) = n, \tag{5.2.8}$$

where the summation extends over all the distinct divisors d of n.

We may now note another property of the additive cyclic group modulo m. Let p be prime; then any integer m can be expressed uniquely in the form

$$m \equiv a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \pmod{p^n}, \tag{5.2.9}$$

where each a belongs in the set $0, 1, \cdots, p-1$. To prove this we may, by Theorem 2.2.8, express m uniquely in the form $m = a_0 + k_1 p$ where a_0 has the required property. We then express k_1 in a similar form, giving $m = a_0 + a_1 p + k_2 p^2$. Proceeding by induction we obtain (5.2.9).

† G. A. Miller, this MONTHLY, vol. 12, 1905, pp. 41–43.

Chapter VI

THE MULTIPLICATIVE GROUP $\mathfrak{G}(m)$ OF RESIDUE CLASSES C_a MODULO m; $(a, m)=1$

6.1. The theorems of Euler and Wilson. We shall now discuss some applications of the results in semigroups we obtained previously. Consider the multiplicative semigroup of residue classes modulo $m>1$. We first note that the set, denoted by $\mathfrak{G}(m)$,

$$C_{r_1}, C_{r_2}, \cdots, C_{r_e}; \qquad (r_i, m) = 1 \tag{6.1.1}$$

with $e=\phi(m)$, forms a group, under multiplication. This follows immediately from Theorem 1.3.4 and Theorem 3.2.2.

We shall now employ the group (6.1.1) and apply Theorem 4.4.9 to it. We find here that for $m>2$, $\phi(m)$ is of the type $2n$, by (5.2.4), so that for a given a with $(a, m)=1$, (4.4.8) becomes for our special group

$$\prod_{i=1}^{e} C_{r_i} = C_{m-1}^{t/2} C_a^d, \tag{6.1.2}$$

where $d=\phi(m)/2$ and where t is the number of solutions in C_x of the relation

$$C_x^2 = C_a, \tag{6.1.3}$$

since there is an element of order two in $\mathfrak{G}(m)$, and it may be taken as C_{m-1}, which is not C_1 for $m>2$.

Let $a=1$; we obtain from (6.1.2)

$$\prod_{i=1}^{e} C_{r_i} = C_{m-1}^{t/2}. \tag{6.1.4}$$

Whence for $m \neq 2$,

$$\prod_{j=1}^{e} r_j \equiv (-1)^{t/2} \pmod{m}, \tag{6.1.5}$$

where t is now the number of incongruent solutions of $x^2 \equiv 1 \pmod{m}$.

Using (6.1.4), (6.1.5) in (6.1.2) gives $C_a^d = C_1$ or C_{m-1} and by squaring, $C_a^{\phi(m)} = C_1$. Whence

$$a^{\phi(m)} \equiv 1 \pmod{m}, \tag{6.1.6}$$

for $m>2$, and it is obvious for $m=2$. This is Euler's generalization of Fermat's theorem:

$$a^{p-1} \equiv 1 \pmod{p}, \tag{6.1.7}$$

which follows from (6.1.6) when $m=p$, a prime, since it is obvious that $\phi(p) = p-1$. Also, if $m=p$ in (6.1.5), we find Wilson's theorem:

$$(6.1.8) \qquad (p-1)! \equiv -1 \pmod{p}$$

since there are not more than two solutions of $x^2 \equiv 1 \pmod{p}$ by the Corollary 4.3.3. Using the known number of solutions in x in $x^2 \equiv 1 \pmod{m}$ in (6.1.5), then we have a generalization of (6.1.8) due to Gauss.

6.2. Criterion for the solution of a quadratic congruence modulo p. Again from (6.1.2) and (6.1.8), with $m=p$, we have $C_a^{(p-1)/2} = C_1$ or C_{p-1} according as $C_x^2 = C_a$ has solutions or has no solutions in C_x; whence

THEOREM 6.2.1. *The congruence*

$$x^2 \equiv a \pmod{p},$$

with p an odd prime and $(a, p)=1$, has solutions or has no solutions in x according as

$$(6.2.2) \qquad a^{(p-1)/2} \equiv \pm 1 \pmod{p}.$$

Putting $a=-1$ in (6.2.2) gives, since p is odd,

$$-1 \equiv (-1)^{(p-1)/2} \pmod{p}$$

when $p \equiv 3 \pmod 4$, and

$$1 \equiv (-1)^{(p-1)/2} \pmod{p}$$

when $p \equiv 1 \pmod 4$, so that

$$(6.2.3) \qquad x^2 \equiv -1 \pmod{p}$$

has solutions if and only if $p \equiv 1 \pmod 4$.

6.3. The Minkowski-Thue theorem on linear congruences. Suppose $m>1$, and $(a, m)=1$, and let k denote the least integer $>\sqrt{m}$. Consider the numbers of the form $(ay+x)$ where x and y each range independently over the set $0, 1, \cdots, k-1$. As $k^2 > m$, then it follows that at least two numbers of this form are congruent modulo m, and we may set

$$ay_1 + x_1 \equiv ay_2 + x_2 \pmod{m},$$

with either $y_1 \neq y_2$ or $x_1 \neq x_2$. Whence

$$(6.3.1) \qquad a(y_1 - y_2) \equiv x_2 - x_1 \pmod{m},$$

with both $x_1 \neq x_2$, $y_1 \neq y_2$, since if either $y_1 = y_2$ or $x_1 = x_2$, with $(a, m)=1$, our assumption, "either $y_1 \neq y_2$ or $x_1 \neq x_2$," is violated. Hence, setting $u = |y_1 - y_2|$, $v = |x_1 - x_2|$, we have

$$(6.3.2) \qquad au \equiv \pm v \pmod{m},$$

with $0 < u \leqq k-1$, $0 < v \leqq k-1$. And we have

THEOREM 6.3.3. (*Minkowski-Thue*).* *Let $m>1$, and let k denote the least integer $>\sqrt{m}$. Then for any given integer a with $(a, m)=1$ we have nonzero integers u and v such that each does not exceed $k-1$, and* (6.3.2) *holds.*

6.4. The expression of $p=4n+1$ as the sum of two squares. Take a as satisfying (6.2.3) in (6.3.2) with $m=p=4n+1$, and square both members of (6.3.2); this gives

$$v^2 + u^2 \equiv 0 \pmod{p} \tag{6.4.1}$$

with $|u|$ and $|v|$ each $<\sqrt{p}$, whence $0<u^2+v^2<2p$, and we have from (6.4.1)

THEOREM 6.4.2 (*Fermat*). *If p is any prime of the form $4n+1$ then*

$$p = a^2 + b^2 \tag{6.4.3}$$

Problem 6.4.4. Prove that the representation (6.4.3) is unique aside from order and sign.

6.5. Repetitive sets with application to Euler's theorem. Consider the distinct elements

$$A_1, A_2, \cdots, A_t \tag{6.5.1}$$

of a finite subset of a commutative semigroup $\mathfrak{S}$ and suppose there exists an element C in $\mathfrak{S}$ such that

$$CA_1, CA_2, \cdots, CA_t \tag{6.5.2}$$

are equivalent in some order to the elements of (6.5.1); then (6.5.1) is called a *repetitive set in $\mathfrak{S}$ with multiplier C.* It is obvious that the set of multipliers of a repetitive set forms a semigroup. It is also clear, by Theorem 1.3.4, that if $\mathfrak{S}$ is finite then the set of all its elements forms a repetitive set with respect to any cancellable element of $\mathfrak{S}$ as a multiplier.

If $\mathfrak{R}$ is a repetitive set and C a multiplier, then C need not be in $\mathfrak{R}$; neither is $\mathfrak{R}$ necessarily a semigroup, as is seen from the example of the set of classes C_2 and C_3 modulo 5, with multiplier C_4. Now C_4 is not in the set; the product C_2C_3 is likewise not in the set, so that the repetitive set in this case does not form a semigroup.

It is possible to generalize this notion. Suppose that the elements of the set (6.5.2) are equal in some order to the distinct elements

$$N_1A_1, N_2A_2, \cdots, N_tA_t \tag{6.5.3}$$

* This theorem has been attributed to Thue, alone, by many writers, but it is a special case of a classical theorem of Minkowski's, which appeared in the year 1896, and this seems to have been some years before Thue published anything on it. *Cf.* Vandiver, Bull. Amer. Math. Soc., vol. 22, 1915, pp. 61–68, where some references are given and where more general congruences of this type were also obtained. *Cf.* also A. Brauer and R. L. Reynolds, Can. Jour. of Math., vol. 3, 1951, pp. 367–374.

where the N's belong to a subsemigroup $\mathfrak{S}'$ of $\mathfrak{S}$. We say then that (6.5.1) is a *repetitive set in $\mathfrak{S}$ with respect to $\mathfrak{S}'$ and with multiplier C.*

Repetitive sets of the type first mentioned are called *ordinary*. If we multiply together the quantities (6.5.3), then we obtain, using (6.5.2)

$$C^t \prod_{i=1}^{t} A_i = \prod_{i=1}^{t} N_i A_i.$$

Now further assume $\mathfrak{S}$ is a cancellative semigroup; then we obtain

$$C^t = \prod_{i=1}^{t} N_i. \tag{6.5.4}$$

Let $\mathfrak{S}$ be a group; then the elements of $\mathfrak{S}$ form an ordinary repetitive set with any element as multiplier. If $A \in \mathfrak{S}$ and $\mathfrak{S}'$ above is taken to be the identity E, (6.5.4) becomes

$$A^n = E \tag{6.5.5}$$

with n the order of the group.

We note that (6.1.1) forms a repetitive set of order $\phi(m)$ with any element of (6.1.1) as multiplier. Consequently by (6.5.5) if $(a, m) = 1$,

$$C_a^{\phi(m)} = C_1; \tag{6.5.6}$$

whence we obtain another proof of Euler's theorem, (6.1.6).

For our present uses we shall in the next few sections develop a few theorems concerning commutative rings and finite groups, particularly cyclic groups.

6.6. A basis theorem for finite Abelian groups.

THEOREM 6.6.1. *Let $a_1 a_2 \cdots a_r = m$ be the order of an Abelian group $\mathfrak{G}$ with the a's prime each to each. Then any element C of $\mathfrak{G}$ may be expressed uniquely as*

$$C = A_1 A_2 \cdots A_r \tag{6.6.2}$$

with

$$A_i^{a_i} = E; \qquad i = 1, 2, \cdots, r, \tag{6.6.3}$$

and with E the identity of $\mathfrak{G}$.

We shall first illustrate the method of proof by assuming $r = 2$ in (6.6.2). We use addition as the group operation as this is convenient here. This means, for example, that if we have, in the multiplicative notation, an expression in $\mathfrak{G}$ like $S^a T^b$, we write it in the additive form as $aS + bT$. Also, in particular, if we have, in the multiplicative form $R^k = E$, then this assumes the additive form $kR = 0$, and if S has order r and $c \equiv d \pmod{r}$, then $cS = dS$. We define A_1 as

(6.6.4) $$A_1 = m_1^{k_1} C$$

and A_2 as

(6.6.5) $$A_2 = m_2^{k_2} C$$

with

$$(m/a_i) = m_i$$

and

$$k_i = \phi(a_i),$$

for $i=1, 2$. If we add (6.6.4) and (6.6.5) we obtain

(6.6.6) $$A_1 + A_2 = C(m_1^{k_1} + m_2^{k_2}).$$

The coefficient of C in the above is congruent to 1, modulo a_1, and is congruent to 1, modulo a_2, by (6.5.6), and by Theorem 3.2.5 it is congruent to 1 modulo $a_1 a_2$, since $(a_1, a_2) = 1$. Hence we have (6.6.2) for $r=2$,

$$C = A_1 + A_2.$$

For r general in (6.6.2) we write

$$A_i = C m_i^{k_i},$$

and proceeding as we did for the case $r=2$, we find

(6.6.7) $$C = C \sum_{i=1}^{r} m_i^{k_i} = \sum_{i=1}^{r} A_i.$$

Now the coefficient of C in the left-hand member is $\equiv 1 \pmod{m}$ since $m_i^{k_i} \equiv 1 \pmod{a_i}$ for $i=1, 2, \cdots, r$, and we may use again the result in Theorem 3.2.5 and the relation (6.5.6). Hence we have (6.6.2). To prove the uniqueness of this representation let us assume another representation of this kind exists so that

$$B_1 + B_2 + \cdots + B_r = A_1 + A_2 + \cdots + A_r;$$

then for each i in the set $1, 2, \cdots, r$, we have

$$m_i^{k_i} \sum_{j=1}^{r} B_j = m_i^{k_i} \sum_{j=1}^{r} A_j,$$

which gives by (6.6.3), written in additive notation,

$$B_i = A_i$$

for any i; whence follows Theorem 6.6.1.

We use the notation employed in the proof of Theorem 6.6.1 relative to a modulus $m = \prod_{i=1}^{r} a_i$ and wish to find an integer s such that for given integers s_i, $i = 1, 2, \cdots, r$, $s \equiv s_i \pmod{a_i}$. We write

$$\sum_{i=1}^{r} m_i^{k_i} s_i, \tag{6.6.8}$$

and we see that this is an s desired. This explicit solution* of the so-called *Chinese problem of reminders* we shall find a powerful tool in much of our remaining work in this paper.

6.7. A criterion for cyclic groups. We shall now obtain further properties of groups. Here we consider any finite group $\mathfrak{F}$ of order n having the property that for every d dividing n then $X^d = E$ has at most d solutions X in $\mathfrak{F}$. Using the same scheme employed in the proof of Theorem 5.2.7, we shall show that $\mathfrak{F}$ is cyclic. If there is a cyclic subgroup $\mathfrak{C} \subset \mathfrak{F}$ of order d, then d divides n, and it has exactly $\phi(d)$ generators by Theorem 1.3.1 and Theorem 5.1.1. Also, there cannot be another cyclic group of order d in $\mathfrak{F}$, otherwise $X^d = E$ would have more than d solutions in $\mathfrak{F}$; *i.e.*, if A is a generator, then $A, A^2, \cdots, A^d$ give distinct solutions. But every element of $\mathfrak{F}$ generates some cyclic subgroup of $\mathfrak{F}$, and there must be a cyclic subgroup of $\mathfrak{F}$ corresponding to each divisor d of n, since if none existed for some d_1 with $n \equiv 0 \pmod{d_1}$, then the order of $\mathfrak{F}$ would be less than n, as a consequence of the relation $\sum_d \phi(d) = n$. Therefore for $d = n$, some element generates $\mathfrak{F}$ itself, which makes $\mathfrak{F}$ cyclic. Conversely, by Theorem 5.1.1, if $\mathfrak{F}$ is cyclic, then $X^d = E$ has no more than the d solutions:

$$B^{n/d}, B^{2n/d}, \cdots, B^{dn/d},$$

where B generates $\mathfrak{F}$. Consequently we may state the

THEOREM† 6.7.1. *A finite group $\mathfrak{F}$ of order n and identity E is cyclic if and only if for every d dividing n the relation*

$$X^d = E$$

has at most d solutions X in $\mathfrak{F}$.

---

* Vandiver, Annals of Math., II, vol. 18, 1917. pp. 115–119, Theorem I. Also, in other publications he used this form in connection with a composite ideal modulus in an algebraic field of which the m related to (6.6.8) is a special case.

† H. Zassenhaus, The Theory of Groups, Chelsea Publishing Co., New York, New York, 1949, p. 74.

6.8. The number of solutions of $ax \equiv b \pmod{m}$, $(a, m) = d$, with application to cyclic groups. We shall now prove

THEOREM 6.8.1. *The congruence*

$$ax \equiv d \pmod{n} \tag{6.8.2}$$

has $(a, n) = r$ incongruent solutions or no solutions according as r does or does not divide d. If it has solutions, then for $a = a_1 r$, $n = kr$, $d = d_1 r$ and t a solution of $a_1 t \equiv d_1 \pmod{k}$, the r solutions are given by

$$t, t + k, \cdots, t + (r - 1)k.$$

Proof. If (6.8.2) is written in the form $ra_1x - d \equiv 0 \pmod{kr}$, we see that it has a solution if r divides d, and not otherwise. Now assume $d = d_1 r$ and write (6.8.2) as $r(a_1x - d_1) \equiv 0 \pmod{rk}$. This has a solution since $a_1x \equiv d_1 \pmod{k}$ has a solution by Theorem 4.2.1 and Corollary 2.2.3. Write this unique solution, t modulo k in the r forms, $x = t + sk$, $s = 0, 1, \cdots, r-1$, each less than n. Clearly these give exactly the incongruent solutions of (6.8.2), since each x which satisfies (6.8.2) also satisfies $a_1x - d_1 \equiv 0 \pmod{k}$, and each $t + sk$ satisfies $r(a_1x - d_1) \equiv 0 \pmod{rk}$ and therefore (6.8.2).

We shall now apply Theorem 6.8.1 to the theory of cyclic groups. Let us consider the solution of $X^a = B$ in a cyclic group $\mathfrak{G}$. Then we may put, if R generates $\mathfrak{G}$, $B = R^d$. We may set also $X = R^y$ with y to be determined. Hence our equation becomes

$$R^{ay} = R^d, \qquad R^{ay-d} = E, \tag{6.8.3}$$

and from Theorem 1.3.1, $ay \equiv d \pmod{n}$ where n is the order of $\mathfrak{G}$. Our problem, then, is to find the values of y which are less than or equal to n, and these are given by Theorem 6.8.1. Hence we have

THEOREM 6.8.4. *In a cyclic group $\mathfrak{G}$ of order n the equation $X^a = R^d$ has r solutions or no solutions X according as r divides d or does not divide d; $r = (a, n)$; R is a generator of $\mathfrak{G}$.*

Note that the group of Theorem 6.8.4 is *abstractly identical* with that of the additive group of residue classes defined by the residues modulo n in Theorem 6.8.1, in the sense that if we identify multiplication in $\mathfrak{G}$ with addition modulo n and the element R^a with C_a, where $0 \leqq a < n$, then these groups have identical operations tables, with respect to multiplication and addition, respectively. Such a relation between two semigroups, and hence groups, is called an *isomorphism*. If each element of the semiring $\mathfrak{S}$ is related to exactly one element of the semiring $\mathfrak{S}'$, and conversely, in such a way that whenever α, $\beta \in \mathfrak{S}$ are related, respectively, to α', $\beta' \in \mathfrak{S}'$, it follows that $\alpha\beta$ and $\alpha + \beta$ are related, respectively, to $\alpha'\beta'$ and $\alpha' + \beta'$; then this relationship is also called an *isomorphism*, and the semirings are said to be *isomorphic*.

6.9. Primitive roots modulo m. Consider the residue classes, modulo p, a prime, excluding the zero class, represented by

$$C_1, C_2, \cdots, C_{p-1}. \tag{6.9.1}$$

These form a group under multiplication of order $p-1$, as we remarked after (6.1.1). For n any divisor of $(p-1)$ the equation $C_x^n = C_1$ has no more than n distinct solutions C_x since the congruence $x^n \equiv 1 \pmod{p}$ has no more than n incongruent solutions, by the Corollary 4.3.3. If we use Theorem 6.7.1 it follows that (6.9.1) forms a cyclic group.

The integer a is said to *belong to the exponent* d, modulo m, if

$$a^d \equiv 1 \pmod{m};$$

but

$$a^k \not\equiv 1 \pmod{m}$$

for $0 < k < d$; in particular if $d = \phi(m)$, then a is said to be a *primitive root* modulo m. We have just proved that at least one primitive root modulo m exists when m is prime.

We note the following result which follows immediately from Theorem 6.8.4.

Let g be a primitive root modulo the prime p; then

$$x^a \equiv g^d \pmod{p}$$

has $r = (a, p-1)$ incongruent solutions or no solution according as r divides d or does not divide d.

This is sometimes called the fundamental theorem of binomial congruences, modulo p.

The question as to primitive roots modulo m, when m is composite, is more complicated. We have by (6.1.6) for $m = p^n$, p prime, a prime to p, for p odd,

$$a^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n}; \tag{6.9.2}$$

so we consider the residue classes, with $e = \phi(p^n)$,

$$C_{r_1}, C_{r_2}, \cdots, C_{r_e}, \tag{6.9.3}$$

where the r's are the integers less than p^n and prime to it. They form a group as we have noted earlier, which we shall now show is cyclic for p odd. It is easy to show that the solutions in a commutative group $\mathfrak{R}$ of order n of the equation $X^r = E$, E the identity of $\mathfrak{R}$, form a group if r divides n. Hence if s divides $p-1$ and $0 \leqq k < n$, each of the sets of solutions of

$$C_x^{sp^k} = C_1, \tag{6.9.4}$$

$$C_y^{s} = C_1, \tag{6.9.5}$$

$$C_z^{p^k} = C_1, \tag{6.9.6}$$

forms a group. Now C_y is a solution of (6.9.5) if and only if

$$y^s \equiv 1 \pmod{p^n}. \tag{6.9.7}$$

By the Corollary 4.3.3 this has no more than s absolutely incongruent solutions in y. Let $a_1, a_2, \cdots, a_h$ be incongruent solutions with $h > s$. Then for some i and j,

$$a_i = a_j + p^t r, \qquad (r, p) = 1 \tag{6.9.8}$$

with $n > t > 0$, and by expansion

$$a_i^s \equiv a_j^s + s a_j^{s-1} p^t r \pmod{p^{t+1}}, \tag{6.9.9}$$

and since $a_i^s \equiv a_j^s \equiv 1 \pmod{p^n}$, we find $s a_j^{s-1} p^t r \equiv 0 \pmod{p^{t+1}}$, or $r \equiv 0 \pmod{p}$, a contradiction. Hence (6.9.5) has no more than s solutions in C_y.

Now consider the solutions in C_z of (6.9.6). C_z is a solution of (6.9.6) if and only if, with $0 \leqq k < n$,

$$z^{p^k} \equiv 1 \pmod{p^n}. \tag{6.9.10}$$

Each solution z of (6.9.10) has the form $z = 1 + t p^v$, $v \geqq 1$, $(t, p) = 1$, or $t = 0$, since by Fermat's theorem, $z^{p^k} \equiv z \pmod{p}$. The relation, since p is odd,

$$(1 + t p^v)^{p^r} \equiv 1 + t p^{r+v} \pmod{p^{r+v+1}} \tag{6.9.11}$$

holds for $r = 1$, as we see when we expand and use Theorem 2.2.7. If (6.9.11) holds for $r \geqq 0$, we see that it will hold for $(r+1)$ in lieu of r by raising each member to the power p. Hence it holds for any $r \geqq 0$. If we set $r = k$ and $v = n - k + c$ in (6.9.11), with c to be determined, we obtain $(1 + t p^{n-k+c})^{p^k} \equiv 1 + t p^{n+c} \pmod{p^{n+c+1}}$.

Hence for $(t, p) = 1$, z satisfies (6.9.10) if and only if $c \geqq 0$. By Theorem 2.2.8, $t = t_1 + p^k g$ with $p^k > t_1 \geqq 0$. We note that $z = 1 + t p^{n-k+c} \equiv 1 + (t_1 + p^k g) p^{n-k+c} \equiv 1 + t_1 p^{n-k+c} \pmod{p^n}$. Hence for all $c \geqq 0$ this cannot have more than the p^k solutions $0, 1, \cdots, p^k - 1$, in t_1, and therefore (6.9.10) has no more than p^k solutions in z.

Now the solutions of (6.9.4) form a group whose order divides $s p^k$ and by Theorem 6.6.1 each such solution is the product of an element which satisfies (6.9.5) by one which satisfies (6.9.6). We have just proved that (6.9.5) has no more than s solutions and (6.9.6) no more than p^k solutions; hence (6.9.4) has no more than $s p^k$ solutions, and by Theorem 6.7.1, the group (6.9.3) is cyclic. Otherwise expressed, for p an odd prime, a primitive root modulo p^n exists.

Obviously primitive roots exist modulo 2 and 4, respectively, but not modulo 2^k with $k > 2$, since $a^2 \equiv 1 \pmod{8}$ for any odd a.

Finally, let $m=2p^n$, where p is an odd prime. Employ a primitive root r modulo p^n. Let g be that one of the numbers r and $r+p^n$ which is odd. If g belongs to the exponent e modulo m, then

$$r^e \equiv g^e \equiv 1 \pmod{p^n},$$

whence e is divisible by $\phi(p^n)=\phi(m)$. But $e \leqq \phi(m)$. Hence $e=\phi(m)$ and g is a primitive root modulo m.

We have already noted that no primitive roots exist for 2^t, $t>2$; however, as before, we designate the group (6.9.3) by $\mathfrak{G}(m)$, and we may complete the proof* of

THEOREM 6.9.12. *The groups* $\mathfrak{G}(2)$, $\mathfrak{G}(4)$, $\mathfrak{G}(p^n)$, $\mathfrak{G}(2p^n)$, p *odd, are cyclic. If* $t \geqq 3$, *then the group* $\mathfrak{G}(2^t)$ *has the property that any given element in it may be expressed in the form* AB *with* A *a unique element in a cyclic group of order* 2, *and* B *a unique element in a cyclic group of order* 2^{t-2}, *where the generators of these cyclic groups are, respectively, the residue classes* C_a, *with* $a \equiv -1 \pmod{2^t}$, *and* C_b, *with* $b \equiv 5 \pmod{2^t}$.

Proof. $\mathfrak{G}(2)$ and $\mathfrak{G}(4)$ are obviously cyclic. $\mathfrak{G}(p^n)$ and $\mathfrak{G}(2p^n)$ were proved cyclic above.

For the proof of the theorem concerning $\mathfrak{G}(2^t)$, $t>2$, we shall first show that

$$5^{2^k} \not\equiv 1 \pmod{2^t} \text{ for } t \geqq 3 \text{ and } k < t-2, \tag{6.9.13}$$

but

$$5^{2^{t-2}} = 1 + 2^t u, \text{ where } u \text{ is odd and } t \geqq 3. \tag{6.9.14}$$

Since $25=1+8\cdot 3$, then the last equation is satisfied by $t=3$. By induction it is true in general, as we observe that

$$5^{2^{t-1}} = (1+2^t u)^2 = 1 + 2^{t+1}u + 2^{2t}u^2 = 1 + 2^{t+1}u(1+2^{t-1}u).$$

Hence we have (6.9.14). Now if 5 belongs to the exponent n modulo 2^t, then n divides 2^{t-1} by Theorem 1.3.1 and (6.5.6). It then follows from (6.9.14) that 5 belongs to the exponent 2^{t-2} modulo 2^t, and we have (6.9.13). We return to the first equation above, and we shall show that if $2^{t-2}=c$, and $t \geqq 3$,

---

* A simpler proof, using group theory, of the fact that primitive roots modulo p^n and $2p^n$ exist when p is odd, may be given by the use of the criterion that an Abelian group of order h is cyclic if and only if for every prime q dividing h, the relation

$$x^q = E,$$

where E is the identity of the group, has exactly q solutions. However, as of now, we know of no proof of this which does not involve the use of the basis theorem for Abelian groups, which we are avoiding in the present work.

$$(6.9.15) \qquad \begin{matrix} 5, 5^2, \cdots, 5^c, \\ -5, -5^2, \cdots, -5^c \end{matrix}$$

give all the 2^{t-1} odd incongruent residues modulo 2^t. Since 5 belongs to 2^{t-2} modulo 2^t, the elements of the first line alone are incongruent modulo 2^t and similarly for the second line. If we have $5^a \equiv -5^b \pmod{2^t}$, a and b each in the range $0, 1, \cdots, c$, then if $a > b$,

$$5^{a-b} \equiv -1 \pmod{2^t}, \qquad 5^{2(a-b)} \equiv 1 \pmod{2^t}.$$

Again, since 5 belongs to the exponent 2^{t-2}, modulo 2^t, then $2(a-b) \equiv 0 \pmod{2^{t-2}}$, $a-b \equiv 0 \pmod{2^{t-3}}$; whence $a-b = 2^{t-3}$, and $5^{2^{t-3}}+1 \equiv 0 \pmod{2^t}$. However, this is impossible since $5^{2^{t-3}}-1 \equiv 0 \pmod 4$; hence $5^{2^{t-3}}+1 \not\equiv 0 \pmod{2^t}$. This proves Theorem 6.9.12, as the generators of the cyclic groups of orders 2 and 2^{t-2} are, respectively, the residue classes determined by (-1) and 5, modulo 2^t.

6.10. A theorem on the cyclic subgroup of $\mathfrak{G}(m)$ of maximal order, with application to Carmichael numbers. Since the above discussion shows that we do not have primitive roots corresponding to all moduli, we may consider the problem of determining the order of a *maximal cyclic group* (a cyclic group of maximum order) contained in $\mathfrak{G}(m)$. This is an extension of the problem of finding primitive roots, as when a primitive root g, $0 \leqq g < m$ exists for a modulus m, then C_g generates the cyclic group of residue classes $\mathfrak{G}(m)$ corresponding to integers prime to m, and this group is maximal. R. D. Carmichael* defined a numerical function $\lambda(m)$ having the following properties:

$$\lambda(2^t) = \phi(2^t) \text{ if } t = 0, 1, 2;$$

$$\lambda(2^t) = \tfrac{1}{2}\phi(2^t) \text{ if } t > 2;$$

$$\lambda(p^t) = \phi(p^t) \text{ if } p \text{ is an odd prime;}$$

$$\lambda(2^t p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}) = h, \text{ with each } p \text{ an odd prime,}$$

where h is the least common multiple of $\lambda(2^t), \lambda(p_1^{t_1}), \cdots, \lambda(p_1^{t_n})$.

We shall now apply some relations used in the proof of Theorem 6.6.1 to the obtaining of results, in effect, in the theory of the additive cyclic group of the residue classes modulo m, as well as in the theory of the multiplicative group $\mathfrak{G}(m)$, where, if the p's are distinct primes,

$$m = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}.$$

If we set $a_i = p_i^{t_i}$ in the statement of Theorem 6.6.1 with $r = n$ and let $\mathfrak{G}$ be the additive group of the residue classes C_a, $a = 0, 1, \cdots, m-1$, then (6.6.7), with the remark following it, gives, using congruences,

---

* Bull. Amer. Math. Soc., vol. 15, 1908–9, pp. 221–222.

$$a \equiv a \sum_{i=1}^{n} (m/p_i^{t_i})^{\phi(p_i^{t_i})} \pmod{m}, \tag{6.10.1}$$

for a given a. Setting

$$a \equiv r_i \pmod{p_i^{t_i}}, \qquad i = 1, 2, \cdots, n, \tag{6.10.2}$$

we obtain

$$a \equiv \sum_{i=1}^{n} r_i (m/p_i^{t_i})^{\phi(p_i^{t_i})} \pmod{m}. \tag{6.10.3}$$

The converse of this result was given in (6.6.8).

Let a belong to the exponent k modulo m, and take (6.10.2) to the kth power and assume that r_i belongs to the exponent e_i modulo $p_i^{t_i}$, $i=1, 2, \cdots, n$. Then we have

$$r_i^k \equiv 1 \pmod{p_i^{t_i}}; \qquad i = 1, 2, \cdots, n. \tag{6.10.4}$$

Hence k is a multiple of e_i, $i=1, 2, \cdots, n$. Suppose in particular that we select an a in (6.10.1) such that r_i belongs to $\lambda(p_i^{t_i})$ for $i=1, 2, \cdots, n$, which is always possible by Theorem 6.9.12. Then k is the L. C. M. of these λ's, which is $\lambda(m)$. Then a belongs to $\lambda(m)$ modulo m, *so that C_a generates a cyclic subgroup of order $\lambda(m)$ in the group of residue classes $\mathfrak{G}(m)$ of* (6.1.1). Further, in the above, the e_i, $i=1, 2, \cdots, n$ are divisors of $\lambda(p_i^{t_i})$, respectively, by Theorem 1.3.1. Consequently we have

$$b^{\lambda(m)} \equiv 1 \pmod{m}, \tag{6.10.5}$$

for any b with $(b, m)=1$. We may then state

THEOREM 6.10.6. *If $\mathfrak{G}(m)$ is the group of residue classes given in* (6.1.1), *then a cyclic subgroup of maximal order has $\lambda(m)$ as its order.*

We shall next apply the above result to the following well-known problem. For what integers n is $a^{n-1} \equiv 1 \pmod{n}$ for all a's such that $(a, n)=1$? Suppose n is such an integer, and let some a, say a_1, belong to the exponent $\lambda(n)$, which is always possible, as we have seen. Then it follows that $n \equiv 1 \pmod{\lambda(n)}$ by Theorem 1.3.1. On the other hand, if $n \equiv 1 \pmod{\lambda(n)}$, then by (6.10.5), if $(a, n)=1$, it follows that $a^{\lambda(n)} \equiv 1 \equiv a^{n-1} \pmod{n}$. So we have the criterion: $a^{n-1} \equiv 1 \pmod{n}$ *for all a's such that $(a, n)=1$, if and only if* $n \equiv 1 \pmod{\lambda(n)}$. Below the number 2,000 there are only three values for composite n, namely, $561 = 3 \cdot 11 \cdot 17$; $1105 = 5 \cdot 13 \cdot 17$; $1729 = 7 \cdot 13 \cdot 19$. Such numbers we shall call *Carmichael numbers*, following the example of several writers.*

* R. D. Carmichael, Bull. Amer. Math. Soc., vol. 16, 1909–10, pp. 237–238; this MONTHLY, vol. 19, 1912, pp. 22–27.

6.11. Integral homogeneous symmetric functions defined over repetitive sets in commutative rings with units. Here we shall discuss a type of function in a commutative finite ring which has a multiplicative identity denoted by 1. We define the *indicator* of $\Re$ as the number of distinct units in its multiplicative semigroup. If $F(\gamma_0, \gamma_1, \cdots, \gamma_j)$ is a function with the γ's in a ring, then F is called an *integral homogeneous symmetric function* of degree d, written IHSF provided it satisfies:

(i) F is a polynomial in the γ's, which is unchanged aside from the order of the terms by any permutation of the γ's.

(ii) $F(\sigma\gamma_0, \sigma\gamma_1, \cdots, \sigma\gamma_j) = \sigma^d F(\gamma_0, \gamma_1, \cdots, \gamma_j)$, $\sigma \in R$.

Consider an IHSF of degree d formed by an ordinary repetitive set,† say

$$F(\beta_1, \beta_2, \cdots, \beta_k).$$

If β is a multiplier of the repetitive set, then

$$F(\beta\beta_1, \beta\beta_2, \cdots, \beta\beta_k) = F = \beta^d F,$$

and

$$(\beta^d - 1)F = 0. \tag{6.11.1}$$

It is easy to show that no unit μ satisfies $\mu F = 0$ for $F \in \Re$, $F \neq 0$. Now if it is possible to select β and d so that $\beta^d - 1$ is a unit in $\Re$, then $F = 0$. This can be done in a number of special cases.

For example, we may consider the application of the above ideas to the residue classes modulo m. We can select many subsets of this system which form repetitive sets and apply the relation (6.11.1) to obtain various results. However, we may obtain theorems giving us more information concerning exceptional cases when we consider the whole ring modulo m.

Under multiplication the set of distinct residue classes modulo m forms a repetitive set with any C_a, $(a, m) = 1$, as multiplier.

Let

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where the p's are distinct primes, and let S be an IHSF of the distinct residue classes modulo m. Then by (ii) above, we have if d is the degree of S and $(b, m) = 1$, $SC_b^d = S$. Hence

$$S(C_b^d - C_1) = 0. \tag{6.11.2}$$

Now assume that d is not a multiple of $\phi(p_i)$, where $\phi(p_i)$ represents the indicator of p_i, $i = 1, 2, \cdots, k$, and let C_{b_i} be such that b_i is a primitive root modulo p_i. Then

† The idea of an ordinary repetitive set in any finite ring was defined in Vandiver, Annals of Math., II, vol. 18, 1916–17, pp. 105–114, and the definition may obviously be extended to finite sets in any ring.

$$d = r\phi(p_i) + d_i,$$

where $0 < d_i < \phi(p_i)$, and we have

$$b_i^{d_i} \not\equiv 1 \pmod{p_i},$$

for $i = 1, 2, \cdots, k$. Then by the Chinese problem of remainders select a c so that

$$c \equiv b_i \pmod{p_i^{a_i}}. \tag{6.11.3}$$

Hence $c^d - 1$ is prime to m if d is not a multiple of $(p_i - 1)$, $i = 1, 2, \cdots, k$, and by (6.11.2), we have the

THEOREM* 6.11.4. *An IHSF of all the distinct residue classes modulo m is equal to the zero class, except possibly when the degree of the function is divisible by one of the integers $(p_i - 1)$, where $i = 1, 2, \cdots, k$, and $p_1, p_2, \cdots, p_k$ are the distinct prime factors of m.*

The reader may easily verify that the above theorem also holds if we restrict the residue classes in the IHSF mentioned to be the set $\mathfrak{G}(m)$.

We also obtain from (6.11.1) the following theorem, which we give without proof:

THEOREM 6.11.5. *Any IHSF of the elements of an ordinary repetitive set in a finite commutative ring $\mathfrak{R}$ with unity element, whose degree is prime to the indicator of $\mathfrak{R}$, is zero in $\mathfrak{R}$, provided there exists a multiplier η of the set such that $\eta(\eta - 1)$ is a unit in $\mathfrak{R}$.*

6.12. Direct product of semigroups with application to $\mathfrak{G}(m)$. We shall now describe the concept of direct products of semigroups. Suppose that a *countable* (that is, such that the non-equivalent elements can be put into one-to-one correspondence with the positive integers) semigroup $\mathfrak{S}$ contains a set of subsemigroups

$$\mathfrak{S}_1, \mathfrak{S}_2, \cdots \tag{6.12.1}$$

such that

(i) $\mathfrak{S}_i$ and $\mathfrak{S}_j$ have at most the identity E, if such exists in $\mathfrak{S}$, in common for $i \neq j$.

(ii) If $S_i \in \mathfrak{S}_i$, $S_j \in \mathfrak{S}_j$, and $i \neq j$, then $S_i S_j = S_j S_i$.

(iii) If $S \in \mathfrak{S}$ then S is expressible in the form, for some m,

---

* *Loc. cit.*, p. 36.

$$S = \prod_{i=1}^{m} S_{k_i},\ S_{k_i} \in \mathfrak{S}_{k_i}, \tag{6.12.2}$$

with each $\mathfrak{S}_{k_i}$ some element in the set (6.12.1) and where such pair of different S_{k_i}'s are contained in different $\mathfrak{S}_{k_i}$'s.

(iv) Whenever an element of $\mathfrak{S}$ has factorizations as in (iii),

$$\prod_{i=1}^{a} S_{e_i} = \prod_{i=1}^{b} S_{d_i}, \tag{6.12.3}$$

where no element in either factorization is the identity for $\mathfrak{S}$, if such exists, then $a = b$, and the S_{e_i}'s are the S_{d_i}'s in some order.

Then $\mathfrak{S}$ is said to be a *direct product** of the semigroups (6.12.1). If the semigroups in (6.12.1) are all cyclic, then a set consisting of a generator for each of the semigroups in (6.12.1) is called a basis† for $\mathfrak{S}$.

Many types of patterns in number theory and algebra are related to these concepts. For example, let us consider again Theorem 2.2.1 and its proof, and we shall show in detail how the decomposition into primes fits into our present scheme and the MSG of positive integers is, in effect, an example of a representation of a semigroup which is a direct product of other semigroups. Our subsets (6.12.1) become in this case the infinite set consisting of the semigroup formed by unity and the cyclic semigroups formed by powers of p where p varies over the set of primes. As each natural number >1 can be expressed as a product of primes, then the remarks concerning (6.12.2) hold. The conditions, in connection with our relation (6.12.3), also hold since factorization is unique; hence in the language we are using at present, Theorem 2.2.1 may be stated in the form, *The semigroup consisting of the natural numbers under multiplication may be expressed as the direct product of subsemigroups consisting of unity, and the cyclic semigroups generated by the primes p where p varies over the set of primes.*

As another example, let us consider $\mathfrak{G}$ of Theorem 6.6.1. This result is equivalent to the theorem that, using the notation in the statement of the theorem, $\mathfrak{G}$ is the direct product of semigroups, or, in this case, of groups of orders $a_1, a_2, \cdots, a_r$ having the property stated in (6.6.3). Here, contrary to what we observed in connection with Theorem 2.2.1, the identity element is an element belonging to each one of the subgroups mentioned. Here, too, the number of subgroups referred to is finite whereas we employed an infinity of subsemigroups in Theorem 2.2.1. Again in Theorem 6.6.1, as is known, the subgroups are not necessarily cyclic, as in Theorem 2.2.1.

---

* The usual definition of *direct product* of groups is a special case of our definition. We also notice that if an identity is adjoined to each of the $\mathfrak{S}_i$'s in our definition which fails to have one, the order of $\mathfrak{S}$ for the finite case is the product of the orders of the $\mathfrak{S}_i$'s.

† Vandiver, Proc. Nat. Acad. Sci., vol. 20, 1934, pp. 583–584, used in effect, a similar definition of basis.

Even in the case where we consider the semigroup formed by the natural numbers under multiplication we can express it as a direct product of subsemigroups in different ways. Instead of taking the identity group as one of the factors in the product, we can consider, say, the whole semigroup as the product of the cyclic subsemigroups defined by each prime except that in the case of the prime 2, we consider the semigroup consisting of all positive powers of 2 together with unity.

As another application of these concepts, we may consider the semigroup formed by the non-zero rational integers, under multiplication. It is not difficult to see that this system forms a cancellative semigroup, which may be expressed as the direct product of the group generated by (-1) and the cyclic semigroups formed by the positive powers of the primes. Here the basis consists of (-1) and the primes.

If we have given a semigroup with operation addition and with a basis, we have a generalization of the idea of linear independence when we consider the coefficients in the forms as belonging to the semiring of natural numbers. By extending the ideas of group operators to semigroups we may extend the domain of the coefficients to other semirings.

We shall now show that $\mathfrak{G}(m)$, the group of residue classes C_a with $(a, m)=1$, can be expressed as the direct product of certain cyclic groups, a special representation which is important in the theory of group characters. In textbooks on number theory and modern algebra this theorem is not usually given except in connection with a discussion of characters. It is given here in direct and complete form without any reference to that theory. To establish the result we shall use congruences instead of the residue classes directly and consider the following number as a modulus:

$$m = 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \tag{6.12.4}$$

where, in the above, each p is an odd prime. Suppose first that $a_0>2$. If $i=1, 2, \cdots, k$, with g_i a primitive root, modulo $p_i^{a_i}$, then, by (6.6.8) there exist integers r_i and s_i such that

$$r_i = g_i + s_i p_i^{a_i}, \qquad r_i = 1 + t_i(m/p_i^{a_i}). \tag{6.12.5}$$

Similarly we have by the proof of Theorem 6.9.12,

$$r_0 = 5 + u \cdot 4 \cdot 2^{a_0-2}, \qquad r_0 = 1 + t_0(m/2^{a_0}), \tag{6.12.6}$$

$$r = -1 + v \cdot 4 \cdot 2^{a_0-2}, \qquad r = 1 + t(m/2^{a_0}). \tag{6.12.7}$$

We shall now show that if we take

$$r^c r_0^{c_0} \cdots r_k^{c_k} \tag{6.12.8}$$

and let c, c_0, and c_i, $i=1, 2, \cdots, k$, range independently, respectively, over 0 and 1; 0, 1, $\cdots$, $2^{a_0-2}-1$; and 0, 1, $\cdots$, $\phi(p_i^{a_i})-1$, then the $\phi(m)$ elements (6.12.8) are congruent modulo m to the $\phi(m)$ integers less than and prime to m. To prove this, suppose that for some d and some e within the ranges for the c's

$$r^{d}r_0^{d_0}\cdots r_k^{d_k} \equiv r^{e}r_0^{e_0}\cdots r_k^{e_k} \pmod{m}. \tag{6.12.9}$$

If we reduce (6.12.9) modulo 2^{a_0}, we obtain by (6.12.6) and (6.12.7),

$$r^{d}r_0^{d_0} \equiv r^{e}r_0^{e_0} \pmod{2^{a_0}}. \tag{6.12.10}$$

Now we know by Theorem 6.9.12 that the residue classes C_h modulo 2^{a_0}, h odd, $a_0>2$ form under multiplication a group which is the direct product of two cyclic groups, one of order 2, generated by C_j, $j=2^{a_0}-1$, and the other of order 2^{a_0-2}, generated by C_5. Using (6.12.6) and (6.12.7) we have, from (6.12.10), because of the ranges of the d's and e's,

$$d = e, \qquad d_0 = e_0. \tag{6.12.11}$$

Now reduce (6.12.9) modulo $p_n^{a_n}$ where n is some integer in the set $1, 2, \cdots, k$. We find from (6.12.5)

$$r^{d_n} \equiv r^{e_n} \pmod{p_n^{a_n}}. \tag{6.12.12}$$

Because of the fact that g_n is a primitive root modulo $p_n^{a_n}$ in (6.12.5) and because of the ranges for the d's and e's, we find $d_n=e_n$, $n=1, 2, \cdots, k$. Hence the two expressions in (6.12.9) are identical, and by having the d's range as stated we obtain the result that the group of residue classes $\mathfrak{G}(m)$ is the direct product of $k+2$ cyclic groups of residue classes, the C_r's with the r's given in (6.12.5), (6.12.6), and (6.12.7) being the generators, since also

$$\phi(m) = \phi(2^{a_0})\prod_{i=1}^{k}\phi(p_i^{a_i}).$$

Let now $a_0=0$. We find by the use of (6.12.5) and the method used above that our $\mathfrak{G}(m)$ is the direct product of just k cyclic groups. If $a_0=1$, then we note that $\phi(m)=\phi(m/2)$ and that we obtain the generators of k cyclic groups by taking r_i odd in each case in (6.12.5) as is always possible.

Now suppose that $a_0=2$ in (6.12.4). We now select an s, $0\leqq s<m-1$,

$$s \equiv -1 \pmod 4, \qquad s \equiv +1 \pmod{m/4}. \tag{6.12.13}$$

Then we see, using our previous methods, that $\mathfrak{G}(m)$ is in the present case the direct product of $k+1$ cyclic groups having the k generators C_{r_i} obtained from (6.12.5) and the single generator C_s obtained from (6.12.13). We may then state the

THEOREM* 6.12.14. *Let m be defined as in* (6.12.4). *The group of residue classes $\mathfrak{G}(m)$ may be expressed as the direct product of cyclic groups as follows: If $a_0=0$, it is the direct product of k cyclic groups, with generators C_{r_i}, and r_i is defined in* (6.12.5). *If $a_0=1$, $\mathfrak{G}(m)$ is again the direct product of k cyclic groups with generators obtained from* (6.12.5), *provided the r_i's are selected as odd. If $a_0=2$, then $\mathfrak{G}(m)$ is the direct product of $k+1$ cyclic groups with k generators obtained from* (6.12.5) *and a single generator obtained from* (6.12.13). *If $a_0>2$ in* (6.12.4), *then our group can be expressed as the direct product of $k+2$ cyclic groups, and the generators may be obtained from* (6.12.5), (6.12.6), *and* (6.12.7).

---

* Theorem 6.12.14 does not in general give the direct product of groups whose orders are all powers of primes, as may be obtained by using the fundamental basis theorem for Abelian groups (not employed in this paper). However, Theorem 6.12.14 may be used as the first step in determining these latter types of subgroups if such determination is desired. *Cf.* Hasse (*loc. cit.*, p. 2), pp. 40–43.

Chapter VII

QUADRATIC RECIPROCITY

7.1. Simple properties of the Legendre symbol. Consider (6.2.2). In view of this criterion we shall find it convenient to introduce the notation which immediately follows.

If p is an odd prime and $(a, p)=1$, then, in view of Theorem 6.2.1 we define the symbol

$$\left(\frac{a}{p}\right)$$

to be ± 1, and also such that

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\ p).$$

The symbol $(\frac{a}{p})$ just defined, which we shall also write as (a/p), is called Legendre's symbol, or the quadratic character of a, modulo p. (Some writers use $(a \mid p)$ for this symbol, rather than $(\frac{a}{p})$, but we prefer the latter, since its properties given in Problem 7.1.2 (below) resemble to some extent properties of ordinary fractions.) We have easily, from this definition, and (6.2.2),

$$\left(\frac{1}{p}\right) = 1, \qquad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{7.1.1}$$

Problem 7.1.2. Prove that, if $(a_1 a_2, p)=1$, p an odd prime, then

$$\left(\frac{a_1 a_2}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right), \tag{7.1.3}$$

$$\left(\frac{a_1}{p}\right) = \left(\frac{a_1 + kp}{p}\right). \tag{7.1.4}$$

To investigate $(\frac{2}{p})$ we consider*

$$2 \times 1,\ 2 \times 2,\ 2 \times 3,\ \cdots,\ 2 \times p' \quad (p' = (p-1)/2),$$

modulo p. Hence if $a=1, 2, \cdots, p'$, the least absolute residue r_a of $2a$ is even if $2a<p/2$ and odd if $2a>p/2$, so that

$$2a \equiv (-1)^{|r_a|} \mid r_a \mid \ (\mathrm{mod}\ p) \tag{7.1.5}$$

where $|r_a| < p/2$. Also, the resulting r's are distinct since the even ones are incongruent and also the odd ones, and $2p' < p$. Multiplying together the p' congruences (7.1.5), we have

$$2^{p'}(p'!) \equiv (-1)^R (p'!) \ (\mathrm{mod}\ p)$$

* This simple proof of (7.1.6) was communicated to Vandiver by Dr. W. L. G. Williams.

where $R=\sum_{r=1}^{p'}|r_s|$, and since $(p'!)$ is prime to p we have

$$2^{p'} \equiv (-1)^{(p^2-1)/8} \pmod{p},$$

since $R=1+2+\cdots+p'=(p^2-1)/8$; and

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}. \tag{7.1.6}$$

As is easily shown, this may be otherwise expressed by saying that the quadratic character of 2 is $(+1)$ if p is of the form $8n+1$ or $8n+7$, and is (-1) if p is of the form $8n+3$ or $8n+5$.

7.2. Gauss' lemma. We shall now use (6.5.4) to prove the following theorem:

THEOREM 7.2.1 (*Gauss' lemma*). *If the negative residues among the least absolute residues of*

$$a, 2a, \cdots, p'a,$$

modulo p, are μ in number then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}. \tag{7.2.2}$$

Let the semigroup $\mathfrak{S}'$ mentioned relative to (6.5.4) consist of the residue classes C_1 and C_{p-1} and

$$C_1, C_2, \cdots, C_{p-1}$$

be the semigroup $\mathfrak{S}$ mentioned there. Then we shall show that

$$C_1, C_2, \cdots, C_{p'},$$

is a repetitive set with respect to the subgroup consisting of C_1 and C_{p-1}, with any C_a, $(a, p)=1$, as multiplier. If we consider

$$C_aC_1, C_aC_2, \cdots, C_aC_{p'},$$

then we write

$$C_aC_s = C_{t_1}$$

with $t_1>p'$. We note that $C_{t_1}=C_{p-1}C_{p-t_1}$.

On the other hand, consider the cases when

$$C_aC_s = C_{t_2}$$

with $t_2<p'$. Then it follows that the $(p-t_1)$'s and the t_2's constitute the integers $1, 2, \cdots, p'$ in some order. For if $p-t_1' \equiv t_2' \pmod{p}$, then $t_1'+t_2' \equiv 0 \pmod{p}$, which is impossible, since each of the t's is $<p/2$. Then Theorem 7.2.1 immediately follows from (6.5.4).

7.3. The law of quadratic reciprocity. We shall now prove (proof due to Zeller-Frobenius*)

THEOREM 7.3.1. (*The Law of Quadratic Reciprocity.*) *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2\cdot(q-1)/2}. \tag{7.3.2}$$

By Theorem 7.2.1 we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+\nu}, \tag{7.3.3}$$

where

$$\left(\frac{q}{p}\right) = (-1)^{\nu},$$

with ν corresponding to μ in Theorem 7.2.1 when p and q are interchanged.

Consider the number of solutions (x, y) of

$$py - qx = s, \tag{7.3.4}$$

where $-q/2<s<p/2$ and $1\leqq x\leqq p'$, $1\leqq y\leqq q'$, and $p'=(p-1)/2$ and $q'=(q-1)/2$. Then we shall show that the number of solutions (x, y) satisfying (7.3.4) is equal to $\mu+\nu$. In (7.3.4)

let λ denote the number of solutions (x, y) such that $s>p/2$;

let μ_1 denote the number of solutions (x, y) such that

$$0 < s < p/2; \tag{7.3.5}$$

let ν_1 denote the number of solutions (x, y) such that

$$0 > s > -q/2; \tag{7.3.6}$$

let σ denote the number of solutions (x, y) such that $s<-q/2$.

Clearly, the totality of solutions (x, y) is $(p-1)/2\cdot(q-1)/2$ so we have

$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \lambda + \mu_1 + \nu_1 + \sigma.$$

---

* This proof, in several ways the simplest known of the theorem, and depending only on Gauss' Lemma, has appeared in a number of texts. However, we have observed, so far, just one text in English that gives it: W. J. LeVeque, Topics in Number Theory, Addison-Wesley Publishing Company, Inc., Reading, Mass., vol. I, 1956, pp. 69–71. Geometric forms of this proof have been given by Hasse (*loc. cit.*, p. 2), pp. 56–57 and pp. 94–95, D. H. Lehmer, this MONTHLY, vol. 64, 1957, pp. 103–106.

But if (x, y) is a solution of (7.3.4) for $-q/2<s_1<p/2$, and $x'=[(p+1)/2]-x$ and $y'=[(q+1)/2]-y$, then we note that (x', y') is also a solution of (7.3.4) for $s=s_2=[(p-q)/2]-s_1$, and s_2 is in the prescribed range for s_1. Also, we note that if (x, y) is a solution such that $s_1>p/2$; then (x', y') is a solution such that $s_2<-q/2$. Hence $\lambda=\sigma$, and

$$\frac{p-1}{2}\cdot\frac{q-1}{2}=\mu_1+\nu_1+2\lambda;$$

so that

$$\frac{p-1}{2}\cdot\frac{q-1}{2}\equiv\mu_1+\nu_1 \pmod 2. \tag{7.3.7}$$

Consider μ_1; then since $0<s<p/2$, if we take x in the range $1, 2, \cdots, p'$, then (7.3.4) gives $py<(q\cdot p/2)+p/2$ or $y<q'+1$. Hence we have $qx\equiv -s \pmod p$ with $s>0$ so that by the definition of μ we have $\mu_1=\mu$. Similarly if we consider ν_1 and take y in the range $1, 2, \cdots, q'$, the same method shows that $x<p'+1$, and we have $py\equiv s \pmod q$ with s negative and $(-s)$ in the range $1, 2, \cdots, q'$. This gives $\nu_1=\nu$. Hence, by (7.3.3) and (7.3.7), we have a proof of Theorem 7.3.1.

Problems

Problem 7.3.8. Prove that if p has the form $1+8n$, or $3+8n$, then there exist integers x and y such that

$$p=x^2+2y^2.$$

Also, if p has any other form, this equation has no solutions.

Problem 7.3.9. Prove the following generalization of Theorem 6.3.3. Let $m>1$ and

$$ef>m, \qquad e>1, \qquad m\geqq f;$$

then for an a with $(a, m)=1$ there exist an x and y such that

$$ay\equiv \pm x \pmod m$$

with

$$0<x<e, \qquad 0<y<f.$$

Problem 7.3.10. Determine the value of (81/257); (37/103); (965/1093). Decide if the following congruences have solutions: $x^2\equiv 15 \pmod{101}$; $7x^2\equiv 3 \pmod{41}$, $x^2\equiv 673 \pmod{1093}$.

Problem 7.3.11. Give another proof* of Theorem 5.2.7 by considering the n expressions

$$\frac{n}{a}, \tag{7.3.12}$$

$a=1, 2, \cdots, n$, and reducing each to its lowest terms. Show that corresponding to each distinct divisor d of n there are $\phi(d)$ such fractions with numerator d.

If p is prime and a solution of $x^2 \equiv a \pmod{p}$ exists, then a is called a quadratic residue of p, otherwise a is called a quadratic nonresidue of p.

Problem 7.3.13. If p is an odd prime and r is a primitive root modulo p, then show that the least nonnegative residues mod p of $r^2, r^4, \cdots, r^{p-1}$ are the quadratic residues of p.

Problem 7.3.14. Prove that if m^2+1 is divisible by an odd prime p, then p is of the form $4n+1$.

Problem 7.3.15. Prove that -3 is a quadratic residue of $p=3n+1$ and a quadratic non-residue of $p=3n-1$.

Problem 7.3.16. If $p=10n+b$ is a prime, for what positive integers b is it true that $(5/p)=1$?

Problem 7.3.17. If $p=44n+b$ is a prime, for what positive integers b is it true that $(11/p)=1$?

Problem 7.3.18. Suppose m is a positive integer greater than 1, a belongs to s modulo m, b belongs to t modulo m, and $(s, t)=1$. Show that ab belongs to st modulo m.

Problem 7.3.19. Suppose m is a positive integer greater than 1 and a belongs to e modulo m. Show that a^s belongs to $e/(e, s)$ modulo m. Use this result to find the primitive roots modulo 19, given that 3 is a primitive root modulo 19.

Problem 7.3.20. Suppose that x is a primitive root modulo the odd prime p such that $(x, p-1)=1$. Does there exist a positive integer y less than p such that

$$y^x \equiv x \pmod{p}? \qquad \text{(R. P. Kelisky)}$$

---

* Note by Vandiver: One day in the year 1928 when I visited Prof. R. Fueter in Zürich he showed me some notes made by a former student of Kummer (whose name I have forgotten) of the latter's lectures on elementary number theory. The proof of our Theorem 5.2.7 indicated in Problem 7.3.11 was included in the notes.

Problem 7.3.21. Suppose that p is an odd prime and $r=(p-1)/2$ is a primitive root modulo p. Show that there exists a positive integer x less than p such that

$$r^x \equiv x \pmod{p}.$$ (R. P. Kelisky—R. C. Osborne)

Problem 7.3.22. The congruence

$$x^n \equiv a \pmod{p}$$

has g solutions or no solutions according as $a^{(p-1)/g}\equiv 1 \pmod{p}$ holds or not; $g=(n, p-1)$, $(a, p)=1$. (Hint: use Theorem 6.8.4.)

Problem 7.3.23. Show that a primitive root r modulo p^n, where p is an odd prime, is also a primitive root modulo p, and conversely, provided p^2 does not divide $(r^{p-1}-1)$.

Problem 7.3.24. Show that if g is a primitive root modulo the odd prime p and if $g^{p-1}-1$ is divisible by p^2, then g is not a primitive root modulo p^n for $n\geqq 2$.

Problem 7.3.25. Show that if g is a primitive root modulo the prime $p=4n+1$, then $(-g)$ is also a primitive root modulo p.

Problem 7.3.26. Show that if g is a primitive root modulo the prime $p=4n+3$, then $(-g)$ belongs to the exponent $(p-1)/2$ modulo p.

Problem 7.3.27. Show that if a belongs to the exponent $(p-1)/2$ for the prime modulus $p=4n+3$, then a is a primitive root modulo p.

Problem 7.3.28. Show that if $p=8n+3$ and $q=(p-1)/2=4n+1$ are both primes, then 2 is a primitive root modulo p.

Chapter VIII

THE SEMIGROUP OF THE NONUNITS OF THE MULTIPLICATIVE SEMIGROUP OF RESIDUE CLASSES MODULO m

8.1. On the groups contained in finite cyclic semigroups. Let A be an element of a semigroup, and suppose that the semigroup of distinct powers of A is finite:

$$A, A^2, \cdots, A^k, \cdots, A^{s-1}, \qquad A^s = A^k, \qquad s > k > 0. \tag{8.1.1}$$

Now it is possible to show that the elements

$$A^k, A^{k+1}, \cdots, A^{s-1} \tag{8.1.2}$$

form a cyclic group* $\mathfrak{G}$. For a proof we note first that if $s-k$, the order of (8.1.2), is 1, $s-k$ has no prime divisors, and $\mathfrak{G}$ is obviously cyclic. Suppose $s-k>1$. We have for $t \geqq 0$

$$A^{s-k}A^{k+t} = A^{s+t} = A^{k+t}.$$

Assume that

$$A^{r(s-k)}A^{k+t} = A^{k+t}. \tag{8.1.3}$$

It then follows that

$$\begin{aligned} A^{(r+1)(s-k)}A^{k+t} &= A^{s-k}A^{r(s-k)}A^{k+t} \\ &= A^{s-k}A^{k+t} \\ &= A^{k+t}. \end{aligned} \tag{8.1.4}$$

Then by induction (8.1.4) holds for all r's. Clearly there exists an n such that $A^{n(s-k)} \in \mathfrak{G}$; so from (8.1.4) $A^{n(s-k)}$ is an identity for $\mathfrak{G}$. We also have

$$\begin{aligned} (A^{n(s-k)+1})^j &= A^{nj(s-k)}A^j = EA^j \\ &= A^{n(s-k)+j}. \end{aligned}$$

And the distinct elements of $\mathfrak{G}$ are $A^{n(s-k)+i}$, $i=1, 2, \cdots, (s-k)$. And for t in the above range, the inverse of $A^{n(s-k)+t}$ is $A^{n(s-k)+s-k-t}$. Hence $\mathfrak{G}$ is a cyclic group.

8.2. The cyclic semigroups generated by nonunit residue classes. The nonunit residue classes modulo m were investigated by Weaver and E. T. Parker.† Some of their properties will be given below.

We first notice that the congruence $ax \equiv 1 \pmod{m}$ has no solutions if and only if a is divisible by a factor of m; hence the nonunits modulo m are the

* F. C. Biesele, An Introduction to the Theory of Semi-Groups, M. A. thesis, The University of Texas, June 1933, p. 9.

† Weaver, Math. Mag., vol. 25, 1952, pp. 125–136; E. T. Parker, Proc. Amer. Math. Soc., vol. 5, 1954, pp. 612–616.

elements whose least positive residues have one or more prime divisors in common with m. Further, $(r_1r_2, m)=1$ if and only if $(r_1, m)=1$ and $(r_2, m)=1$. Hence the nonunits modulo m form a semigroup under multiplication.

We wish to discuss the order and period of a nonunit class C_t modulo m. We first consider an example. Let $m=24$ and $C_t=C_{10}$. Then (8.1.1) becomes C_{10}, $(C_{10})^2=C_4$, $(C_{10})^3=C_{16}$, with $(C_{10})^4=(C_{10})^3$. C_{10} has period 1 and order 3. We observe that if we write the decomposition of 24 into primes: $24=2^3\cdot 3$, the period n of C_{10} is the exponent to which 10 belongs modulo $(24/2^3)=3$, and if j is the least power of 10 which 2^3 divides, then the order of C_{10} is $j+n-1$. These properties of C_{10} modulo m are general and are stated below as Theorem 8.2.3.

If l is an integer and b is the least positive integer such that $l^b\equiv 0 \pmod d$, then b is called the nullifying exponent of l modulo d. In the above, $b=j$.

We return to the question of the order and period of the nonunit C_t. Let $m=m_1k$, with $(m_1, k)=1$ where each prime divisor of m which divides one of the pair t, k divides the other also. Let b be the nullifying exponent of t modulo k and t belong to n modulo m_1. Then allowing 1 as a possible modulus in the congruences below, we have

$$t^b \equiv 0 \pmod k, \qquad t^n \equiv 1 \pmod{m_1}; \tag{8.2.1}$$

whence

$$t^b(t^n-1) \equiv 0 \pmod{m_1k}, \qquad t^{b+n} \equiv t^b \pmod m. \tag{8.2.2}$$

On the other hand if t has order b_1+n_1-1 and period n_1, we have $t^{b_1}(t^{n_1}-1)$ divisible by km_1 and by Corollary 2.2.3,

$$t^{b_1} \equiv 0 \pmod k, \qquad t^{n_1} \equiv 1 \pmod{m_1}.$$

Hence, by definition of b and n, $b_1 \geqq b$, $n_1 \geqq n$, but by definition of order and period, $b_1+n_1 \leqq b+n$. Therefore $b_1=b$ and $n_1=n$. We have proved

THEOREM* 8.2.3. *Let C_t be a nonunit modulo m, with $m=m_1k$ and $(m_1, k)=1$ where each prime divisor of m which divides one of the pair t, k divides the other also; then if b is the nullifying exponent of t modulo k and t belongs to n modulo m_1, C_t has period n and order $b+n-1$.*

The reader will find it interesting to illustrate the theorem with $m=36$ and $t=2, 10, 9, 18$.

8.3. Unique factorization modulo m. Earlier, we defined direct product in such a way that we had a unique representation (6.12.2) of each element of $\mathfrak{S}$. We wish to extend this notion of unique representation. To do this, we first define the idea of associates, and extend the definition of prime.

---

* This proof is a simplification of the proofs of Theorems 3 and 4 in Weaver (*loc. cit.*, p. 48), pp. 130–131, both of which results are included in our present Theorem 8.2.3.

Let $\mathfrak{S}$ be a commutative semigroup with $\mathfrak{U}$ as its non-null subgroup of units. If $S \in \mathfrak{S}$, the elements $S \cdot U$, where U varies over $\mathfrak{U}$ are called *associates* of one another. S is obviously an associate of itself. If P is a nonunit of $\mathfrak{S}$ such that P has only its own associates for nonunit divisors, then P is called a *prime* of $\mathfrak{S}$.

$\mathfrak{S}$ is called *uniquely factorable, aside from unit elements*, if

(i) $\mathfrak{S}$ contains a subset $\mathfrak{P}$ of primes.

(ii) Each nonunit of $\mathfrak{S}$ is expressible as a product of a unit and powers of distinct primes.

(iii) If N is a nonunit of $\mathfrak{S}$ and $N = U\prod_{i=1}^{r} P_i^{a_i} = V\prod_{j=1}^{s} Q_j^{\beta_j}$ are factorizations of N with U and V units and the P_i's and Q_j's, distinct primes, respectively, then $r = s$ and each $P_i^{a_i}$ is an associate of some $Q_j^{\beta_j}$.

We emphasize from our definition that this factorization is unique only up to associates of the powers of the primes.

If p is a natural prime divisor of the modulus m, and $pu \equiv s_1 \pmod{m}$ for C_u a unit, then $(s_1, m) = p$; hence the residue class containing s_1 is divisible only by associates of that containing p, and by unit classes, and the class containing s_1 is a prime as defined above. However, if C_q is a prime, then since C_q has only its own associates for nonunit divisors, it follows that $(q, m) = p'$ where p' is a natural prime divisor of m, and C_q is an associate of a class containing a natural prime divisor of m. Hence the set $\mathfrak{P}$ of primes P modulo m is the set consisting of the associates of each class containing a natural prime divisor of m.

Since the least positive residues modulo m represent a complete set of residue classes, it follows from arithmetic unique factorization that each nonunit element of the ring of residue classes modulo m can be factored into a unit multiplied by powers of distinct primes.

Next we prove the

LEMMA 8.3.1. *If p^b, for $b > 0$, is the largest power of the natural prime p which divides m, then no two distinct elements of the set C_p, $(C_p)^2$, $\cdots$, $(C_p)^b$ are associates. If there are other elements in the semigroup generated by C_p, they are associates of $(C_p)^b$.*

If p^i and p^j are contained in associated classes, where $1 \leqq j \leqq i \leqq b$, then for some $C_g \in \mathfrak{U}$,

$$p^i \equiv gp^j \pmod{m}, \qquad p^{i-j}g^{-1} \equiv 1 \pmod{m/(p^j, m)},$$

and p^{i-j} is contained in a unit class modulo $m/(p^j, m)$. But since $j \leqq i \leqq b$ it follows that $i = j$, and no two distinct elements of the set C_p, $(C_p)^2$, $\cdots$, $(C_p)^b$ are associates. To prove the second part of the lemma, we note first that if $m = p^b m_1$, $(p, m_1) = 1$ and $m_1 \neq 1$, let $u_1 = m_1 + p$. Then $(u_1, m_1) = (u_1, p) = 1$, and

$(u_1, m) = 1$; consequently u_1 is in a unit class. Therefore by multiplying together $p^b = p^b$ and $u_1^i = (m_1 + p)^i$ we obtain

$$p^{b+i} \equiv (u_1)^i p^b \pmod{m}$$

for $i \geqq 1$.

To prove that each nonunit C_n of the multiplicative semigroup modulo m satisfies (iii), let C_n have the factorizations as in (ii):

$$V \prod_{i=1}^{x} P_i^{a_i} = W \prod_{j=1}^{y} Q_j^{b_j}. \tag{8.3.2}$$

Since for each P_i and Q_j, natural prime divisors p_i and q_j of m and integers contained in unit classes v_i and w_j exist such that $p_i^{a_i} v_i$ and $q_j^{b_j} w_j$ are contained in $P_i^{a_i}$ and $Q_j^{b_j}$, respectively, (8.3.2) gives

$$v \prod_{i=1}^{x} p_i^{a_i} v_i \equiv w \prod_{j=1}^{y} q_j^{b_j} w_j \pmod{m}, \tag{8.3.3}$$

with v, w contained in units. We see that each natural prime that divides one member of (8.3.3) divides the other also, and we may assume that $x = y$ and that (8.3.3) is written in such an order that $p_i = q_j$ when subscripts are $=$, and it follows from the lemma that if $a_i \geqq b_i \geqq b$ where p_i^b is the largest power of p_i dividing m, then $p_i^{a_i} v_i$ and $p_i^{b_i} w_i$ are contained in associated classes. On the other hand, if $a_i \leqq b_i \leqq b$, we can write a congruence from the two members of (8.3.3):

$$p_i^{a_i} e \equiv p_i^{b_i} f \pmod{m},$$

where $(p_i, e) = (p_i, f) = 1$. Hence

$$e \equiv p_i^{b_i - a_i} f \pmod{m/(p_i^{a_i}, m)},$$

and $b_i = a_i$ since p_i divides $m/(p_i^{a_i}, m)$ for $a_i < b$. And C_n has a unique factorization into primes and we have

THEOREM* 8.3.4. *The residue classes modulo m, $m > 1$, form a uniquely factorable multiplicative semigroup, aside from unit divisors.*

* Weaver, Math. Mag., vol. 25, 1952, pp. 132–134.

Chapter IX

THE SEMIRING FORMED BY CERTAIN GENERALIZED RESIDUE CLASSES

9.1. Some finite commutative semirings. In another paper† the foundations of a theory of certain semirings were developed, and a set of postulates was given which covered not only these finite semirings but also the elementary arithmetic of the natural numbers itself. First the set of natural numbers was defined in the usual way. We then considered the infinite set of symbols:

$$A_1, A_2, A_3, \cdots. \tag{9.1.1}$$

We next introduced six postulates to cover the ideas of identity, equality, parentheses, substitution, induction, addition, and multiplication. Concerning the set (9.1.1), we initially made no statements whatever concerning possible equality between members of it. Then, using our postulates, we proved that this system formed a semiring. At no time in the proofs of these theorems did we assume that elements of the set (9.1.1) were distinct; we were free to make any assumption we pleased concerning equality or inequality among the set of elements. We then introduced inequality for the first time and used the symbol $\neq$.

We next considered the set (9.1.1) together with the six postulates, and assumed that for some natural number, not 1, and denoted by m, we had, if m' is the immediate successor of m in the set of natural numbers,

$$A_{m'} = A_1, \tag{9.1.2}$$

under the assumption that

$$A_1 \neq A_k, \tag{9.1.3}$$

if k denotes a natural number in the set

$$2, 3, \cdots, m.$$

We then proved

$$A_k + A_m = A_k; \tag{9.1.4}$$

that is, A_m acted as an additive identity in our set (9.1.1) under addition. We also obtained

$$A_k A_m = A_m A_k = A_m. \tag{9.1.5}$$

It is easy to show that the set (9.1.1), with the conditions (9.1.2), (9.1.3), and (9.1.4) holding, *is isomorphic with the set of residue classes modulo m as defined in* (4.1.1). As we have already noted, this set forms a ring.

† Vandiver, Math. Mag., vol. 1952, pp. 233–250. In the present paper we do not give proofs of the results stated from here on.

9.2. The generalized residue classes. We shall now discuss a semiring which, from our present viewpoint, is an extension of this ring of residue classes. Refer to the set (9.1.1) and assume that

$$A_1, A_2, A_3, A_4, A_5, A_6$$

are unequal, but that $A_7 = A_3$, and that the six postulates mentioned above still hold; then it follows that

$$A_6 + A_1 = A_2 + A_1.$$

Yet we cannot cancel the A_1's; that is, the law of cancellation under addition does not hold in this algebra.

In (9.1.1) the elements repeat in cycles, relative to addition, the elements in each cycle equaling A_3, A_4, A_5, and A_6 in order. There is no element having the property of the zero element. Also, the cancellation law of multiplication does not hold in general. Further, what corresponds to division is not always possible. This semiring cannot be *imbedded* in a ring (a semiring is said to be imbedded in another if it is isomorphic to a subsemiring of the latter), and hence the ring is not the fundamental system for associative distributive algebra. *But from the point of view we have employed here, the semiring just defined is a natural extension of the ring of residue classes*; in fact if we take the elements of the cycle, A_3, A_4, A_5, A_6, and combine them under addition and multiplication subject to the condition $A_7 = A_3$, we have a ring isomorphic to the ring of residue classes modulo 4.

Suppose we consider the set (9.1.1) again and assume $A_1, A_2, \cdots, A_{j-1}$ are distinct but that $A_j = A_i$ for some $i < j$. A semiring of the type just discussed exists for any such i and j. Such semirings reduce to rings only when $i = 1$. These systems have so far been studied very little, although the theory of semirings in general is now receiving considerable attention from investigators.

The Slaught Memorial Papers

The Herbert Ellsworth Slaught Memorial Papers are a series of brief expository pamphlets (paper bound) published as supplements to the American Mathematical Monthly. The following six numbers have already been published:

1. *Fourier's Series, The Genesis and Evolution of a Theory* by R. E. Langer. v + 86 pages.

2. *Outline of the History of Mathematics (6th edition)* by R. C. Archibald. iv + 114 pages.

3. *Proceedings of the Symposium on Special Topics in Applied Mathematics.* Nine articles by various authors. iv + 73 pages.

4. *Contributions to Geometry.* Eight articles by various authors. iv + 75 pages.

5. *The Conjugate Coordinate System for Plane Euclidean Geometry* by W. B. Carver. vi + 86 pages.

6. *To Lester R. Ford on His Seventieth Birthday.* A collection of fourteen articles. vi + 106 pages.

Copies at one dollar each postpaid may be ordered from:

HARRY M. GEHMAN, *Secretary-Treasurer*

MATHEMATICAL ASSOCIATION OF AMERICA
University of Buffalo
Buffalo 14, New York

The Mathematical Association of America

●

The Association is a national organization of persons interested in mathematics at the college level. It was organized at Columbus, Ohio, in December 1915 with 1045 individual charter members and was incorporated in the State of Illinois on September 8, 1920. Its present membership is over 7700, including more than 200 members residing in foreign countries.

Any person interested in the field of mathematics is eligible for election to membership. Annual dues of $5.00 includes a subscription to the *American Mathematical Monthly*. Members are also entitled to reduced rates for purchases of the Carus Mathematical Monographs and for subscriptions to several journals.

Further information about the Association, its publications and its activities may be obtained by writing to:

H. M. GEHMAN, *Secretary-Treasurer*
THE MATHEMATICAL ASSOCIATION OF AMERICA
University of Buffalo
Buffalo 14, New York

PROFESSIONAL OPPORTUNITIES IN MATHEMATICS

Third Edition—January 1958

The Teacher of Mathematics; Opportunities in Mathematical and Applied Statistics; The Mathematician in Industry; Mathematicians in Government; Opportunities in the Actuarial Profession; Non-Academic Employment of Mathematicians; References for Further Reading.

24 pages, paper covers

MATHEMATICAL EDUCATION IN THE U.S.S.R.

By B. V. GNEDENKO

General aspects; Content of the school course; Mathematical Olympiads; Sample problems; The training of mathematicians in the universities; The graduate school.

20 pages, paper covers

$.25 for single copies of either booklet; $.20 each for orders of five or more (any assortment)

Send orders with remittance to:

HARRY M. GEHMAN, *Secretary-Treasurer*
Mathematical Association of America
University of Buffalo
Buffalo 14, New York

THE AMERICAN MATHEMATICAL MONTHLY

Back Numbers

Complete volumes from volume 26 (1919) to volume 64 (1957) inclusive, are for sale at $10 per volume. The Association will pay transportation charges if payment accompanies order.

Harry M. Gehman, *Secretary-Treasurer*
MATHEMATICAL ASSOCIATION OF AMERICA
University of Buffalo
Buffalo 14, New York

Index of Volumes 1 to 56 Inclusive

The American Mathematical Monthly

Copies at one dollar each postpaid may be ordered from:

H. M. Gehman, Secretary-Treasurer
Mathematical Association of America

University of Buffalo **Buffalo 14, New York**

THE OTTO DUNKEL MEMORIAL PROBLEM BOOK

Edited by

HOWARD EVES AND E. P. STARKE

Partial Table of Contents

The Monthly Problem Departments, 1894-1954
The Four Hundred "Best" Problems
A Classification of Monthly Problems
Index of Problems

Copies at one dollar each postpaid may be ordered from:

HARRY M. GEHMAN, *Secretary-Treasurer*

MATHEMATICAL ASSOCIATION OF AMERICA
University of Buffalo
Buffalo 14, New York